The document is intended for unlimited distribution in its unmodified form.
Commercial/production use or distribution requires expressed permission by the author.
Comments or suggestions are welcomed and encouraged.

If you are interested in the release version of this document (which allows editing and printing) sent directly to you via email (and free updates for as long as it is published), send your email address and $15 US to:

Micheal Espinola Jr.
189 N. Policy Rd.
Salem NH, 03079-1986

THE HARDENING OF

Microsoft® Windows NT®

Operating System Version 4.0

REV I

Written by
Micheal Espinola Jr
micheale@ix.netcom.com

COPYRIGHT © MARCH 27, 1998

Santeria™ Systems

the Table of Contents

the Introduction 3
the Hardening 4
Install the Latest Service Pack and Hot-Fixes *4*
Secure the Registry *6*
Secure the Directory and File Structure *8*
Secure the Security Account Manager Database *12*
Secure Client/Server Communications *14*
Secure Event Log Viewing *15*
Secure Performance Data *15*
Secure Print Driver Installation *16*
Secure Services for an Internet or Firewall Server *16*
Secure Unnecessary Network Bindings *19*
Restrict Access to the Schedule Service *20*
Restrict Anonymous Network Access *20*
Restrict Anonymous Network Access from Listing Account Names and Network Shares *21*
Restrict Default Access Controls on Registry Keys *21*
Restrict Client-Side LanManager Password Authentication *22*
Auditing *23*
Audit the System *25*
Audit Base Objects *25*
Audit Privileges *26*
Disable Automatic Administrative Shares *27*
Disable Caching of Logon Credentials *27*
Disable Display of Last User Name *28*
Disable Guest Account *28*
Disable Removable Disk Access from Network *28*
Disable Shutdown Without Logon *29*
Logging Off or Locking the System *29*
Rename the Administrator Account *30*
Wipe the Page File at a Clean System Shutdown *30*
the Network Security Policy 31
Customize the Logon *31*
Enforce Strong User Passwords *32*
Internet Usage and Security Policy Template *33*
the Reference Appendix 36
[A] Default NT Settings *36*
[B] Software Installation Subkey Locations *38*
[C] C2 and the Trusted Computer System Evaluation Criteria *39*
[D] NetBIOS Names *41*
[E] Port Assignments *43*
the Resource Kit Utilities 56
the Glossary 70
the Acknowledgements 73
the Author 74
the Disclaimer 75

THE INTRODUCTION

Preliminary

This security overview and checklist was developed for NT Administrators installing Windows NT Workstation (NTW) or Server (NTS) version 4.0 on a host that requires more security than in its Commercial Off-The-Shelf (COTS) state. It has been designed and formulated with the USA versions of Service Packs and Hot-Fixes in mind. This is not a cultural bias, but an unfortunate representation of Microsoft's misguided development standards for their products in relation to non-domestic (not of the United States and Canada) countries. Every Service Pack and Hot-Fix is available in the USA versions, so these make an obvious choice to base this document against.

Throughout this document, the author has attempted to culminate as many details as possible directly from Microsoft resources, and reference any relevant Knowledge Base articles. With the combination of genuine Microsoft technical specifications and the personal opinions gathered from the numerous IT professionals that have participated in the creation of this document, it is the authors hope that this document will prove to be a valuable, useful tool.

Notice

Administrators preparing to use this document as a systematic check-list for the "Hardening" of their NT installations should have a high degree of familiarity with the Windows NT Operating System and of network security concepts.

Prerequisite

One particular installation's requirements can differ significantly from another. Therefore, it is necessary for administrators to individually evaluate their particular environments and requirements before implementing any of the security configurations suggested within this document. Implementing security settings can affect system configurations already in use or effect requirement variations in the future. Certain applications installed on Windows NT require more relaxed settings to function properly than others because of the nature of the product. Administrators are strongly advised to carefully evaluate recommendations in the context of their system configurations and environment.

Conceptual Misrepresentations

The Microsoft Windows NT Operating System (OS) provides several security features. However, the default COTS configuration is relaxed, especially on the NTW product. Because of the higher availability of NTW to an average home user, using the product in a static/isolated environment, the default configuration has few of the security features enabled. NTS, a higher-end product intended for corporate use, has many features enabled, but not all. Many of the features that can be set require undocumented and manually edited changes of the Registry or the use of utilities found only in the Resource Kits.

Caution

Because of the sensitive nature of the registry, it is highly recommended that non-experienced users do not attempt to edit the Registry. To make a mistake could render the Windows NT OS unusable.

As a precautionary measure before performing any Registry changes, create/update your Emergency Repair Disk information. Ii a mistake is made, you may require the information to restore your installation to its prior configuration.

Information

Refer to Knowledge Base Article ID: Q122857 for more details on using RDISK.

Install the Latest Service Pack and Hot-Fixes

Completed ☐
Not applicable ☐
Not implemented ☐

Service Packs (SP) are means by which Windows NT product updates are distributed to customers. Service Packs keep the product current, and extend and update your computer's functionality so you'll never have to worry about becoming out of date. They include updates, system administration tools, additional components, and drivers, all conveniently bundled for easy downloading.

In between the release of Service Packs, Microsoft releases Hot-Fixes (HF) to address immediate and serious problems with the software that cannot wait for the next Service Pack release. Each Service Pack is a culmination of all of the Hot-Fixes and Service Packs before it.

Install the latest Service Pack and applicable Hot-Fixes. Although not all Hot-Fixes are necessarily required (dependent on your network and/or application needs), Hot-Fixes must be installed in order by ascending date. This is necessary because some later Hot-Fixes replace files used by earlier ones. You may find the latest releases and versions at the following locations:

SP's: http://support.microsoft.com/support/downloads/
HF's: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40

Reminder

If after installing any Service Pack and applicable Hot-Fixes, you add any computer or network services, you must reinstall the Service Pack and Hot-Fixes per their individual installation instructions.

The following pages are the current Service Pack and Hot-Fixes from the date of this documents release:

Name	KB ID's	Date	Title	
nt4sp3	Q152841	97/09/30	Windows NT 4.0 Service Pack 3	☐
oob-fix	Q143478	97/05/22	Stop 0A in TCPIP.SYS When Receiving Out Of Band (OOB) Data	☐
asp-fix	Q165335	97/05/28	Active Server Pages: Progressive Memory Leak	☐
java-fix	Q168748	97/05/28	Java Applets Cause IE 3.02 to Stop Responding w/ SP3	☐
dns-fix	Q142047 Q154984 Q154985 Q167629 Q169461	97/06/09	Bad Network Packet May Cause Access Violation (AV) on DNS Serv	☐
iis-fix	Q143484	97/06/20	IIS Services Stop with Large Client Requests	☐
lsa-fix	Q154087	97/06/25	Access Violation in LSASS.EXE Due to Incorrect Buffer Size	☐
dblclick-fix	Q170510	97/06/30	Double-Clicking the Mouse Button Acts as a Single Click	☐
icmp-fix	Q143478 Q154174	97/07/01	Invalid ICMP Datagram Fragments Hang Windows NT, Windows 95	☐

lm-fix	***Q147706***	97/07/11	How to Disable LM Authentication on Windows NT	☐
zip-fix	***Q154094***	97/07/14	Using Iomega ATAPI Zip Drives with Windows NT	☐
getadmin-fix	***Q146965*** ***Q168748*** ***Q170510***	97/07/15	GetAdmin Utility Grants Users Administrative Rights	☐
winsupd-fix	***Q155701***	97/08/07	Invalid UDP Frames May Cause WINS to Terminate	☐
ndis-fix	***Q156655***	97/08/08	Memory Leak and STOP Screens Using Intermediate NDIS Drivers	☐
scsi-fix	***Q171295***	97/09/05	Fault Tolerant Systems May Encounter Problems with WinNT SP3	☐
simptcp-fix	***Q154460***	97/11/01	Denial of Service Attack Against WinNT Simple TCP/IP Services	☐
2gcrash	***Q173277***	97/11/01	No Memory.dmp File Created with RAM Above 1.7 GB	☐
ide-fix	***Q153296***	97/11/18	Write Cache on IDE/ATAPI Disks Is Not Flushed on Shut Down	☐
wan-fix	***Q163251***	97/11/20	STOP 0xA Due to Buffer Overflow in NDISWAN.SYS	☐
land-fix	***Q165005*** ***Q177539***	97/11/26	Windows Slows Down Due to Land Attack	☐
roll-up	***Q147222***	97/12/11	Group of Hot-Fixes for Exchange 5.5 and IIS 4.0	☐
SAG-fix	***Q177471***	97/12/11	EBCDIC Characters not Properly Converted to ANSI Characters	☐
joystick-fix	***Q177668***	97/12/11	Calibration Does Not Change When You Calibrate Foot Pedals	☐
iis4-fix	***Q169274***	97/12/12	TCP/IP Causes Time Wait States to Exceed Four Minutes	☐
teardrop2-fix	***Q179129***	98/01/09 20:23	STOP 0x0000000A or 0x00000019 Due to Modified Teardrop Attack	☐
tapi21-fix	***Q179187***	98/01/12 : 18:29	Problems Using TAPI 2.1	☐
pcm-fix	***Q180532***	98/02/11 : 17:10	Xircom PC Card Fails to Function	☐
srv-fix	***Q180963***	98/02/12 : 18:24	Denial of Service Attack Causes Windows NT Systems to Restart	☐
pent-fix	***Q163852***	98/02/27 : 20:43	Invalid Operand with Locked CMPXCHG8B Instruction	☐
N/A at time of release	***Q175093***		User Manager Does Not Recognize February 2000 As a Leap Year	☐

Secure the Registry

Completed	☐
Not applicable	☐
Not implemented	☐

All the initialization and configuration information used by Windows NT is stored in the Registry. Normally, the keys in the Registry are changed indirectly, through administrative tools such as the Control Panel or Resource Kit utilities. These methods are recommended. The Registry can also be altered directly, with the Registry Editor. In some instances, there is no other way to change a Registry setting.

The Registry Editor supports remote access to the Windows NT Registry. To restrict network access to the Registry, create the following Registry key and apply appropriate permission to it.

Windows NT supports accessing a remote Registry via the Registry Editor and also through the RegConnectRegistry() Win32 API call. The default security on the Registry allows for easy use and configuration by users in a network. In some cases, it may be useful to regulate who has remote access to the Registry, in order to prevent potential security problems.

The security permissions set on this key will define which users or groups can connect to the system for remote Registry access. The default Windows NT Workstation installation does not define this key and does not restrict remote access to the Registry. Windows NT Server permits only administrators remote access to the Registry.

Warning

Using Registry Editor incorrectly can cause serious, system- wide problems that may require you to reinstall Windows NT to correct them. Microsoft cannot guarantee that any problems resulting from the use of Registry Editor can be solved. Use this tool at your own risk.

The security settings on the following Registry key dictates which User Groups can access the Registry remotely.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentcontrolSet\Control\SecurePipeServers\winreg

The following optional Subkey defines specific paths into the Registry that are allowed access, regardless of the security on the winreg Registry key:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentcontrolSet\Control\SecurePipeServers\winreg\AllowedPaths
Value	Machine
Type	REG_MULTI_SZ

Information

Refer to Knowledge Base Article ID: Q155363 for more details.

Two Registry editing programs (with varying functionality) are included with NT 4.0:

`regedit.exe`	Windows 95/NT interface and icons Allows search for keys, values and data Does not allow you to set permissions, set auditing or take ownership
`regedt32.exe`	Windows 3.1x/3.51 interface and icons. Allows search for keys only Allows you to set permissions, auditing and take ownership

Both will allow you to make changes to Registry information, but the interface and ability to search vary between the two. Using both in concert can making finding data and setting permissions much easier than using them alone.

The following list provides the minimum settings for C2 level registry security as specified in the Department of Justice's "Trusted Computer System Evaluation Criteria", also known as the Orange Book:

Access Types:

Character	*Registry Access*
QV	Query Value
SV	Set Value
CS	Create Subkey
ES	Enumerate Subkey
NT	Notify
CL	Create Link
DE	Delete
RC	Read Control
WD	Write DAC
WO	Write Owner

Access Combination Types:

Access Name	*Directory Access*
None	No Access
Full	QV,SV,CS,ES,NT,CL,DE,WD,WO,RC
Read	QV,ES,NT,RC

Registry Key	*Permissions*	
`HKEY_LOCAL_MACHINE\` `SOFTWARE`	Administrators: Full CREATOR OWNER: Full Everyone: QV,SV,CS,ES,NT,DE,RC SYSTEM: Full	Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Classes`
(and subkeys)
	Administrators: Full
	CREATOR OWNER: Full
	Everyone: QV,SV,CS,ES,NT,DE,RC
	SYSTEM: Full
		Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Description`
(and subkeys)
	Administrators: Full
	CREATOR OWNER: Full
	Everyone: QV,SV,CS,ES,NT,DE,RC
	SYSTEM: Full
		Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Microsoft`
(and subkeys)
	Administrators: Full
	CREATOR OWNER: Full
	Everyone: QV,SV,CS,ES,NT,DE,RC
	SYSTEM: Full
		Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Program Groups`
	Administrators: Full
	CREATOR OWNER: Full
	Everyone: Read
	Power Users: QV,SV,CS,ES,NT,DE,RC
	SYSTEM: Full
		Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Secure`
	Administrators: Full
	Everyone: Read
	CREATOR OWNER: Full
	SYSTEM: Full
		Applied ☐

`HKEY_LOCAL_MACHINE\`
`SOFTWARE\`
`Windows 3.1`
`Migration Status`
	Administrators: Full
	Everyone: Read
	CREATOR OWNER: Full
	SYSTEM: Full
		Applied ☐

Secure the Directory and File Structure

Completed ☐

Not applicable ☐

Not implemented ☐

Make certain that at least your boot partition is New Technology File System (NTFS) format. It is advisable that any attached Hard Disk Drives (HDD) be formatted in NTFS as well. If you need to convert the volume to NTFS, use the `convert.exe` utility to safely reformat the volume into NTFS without disturbing the existing file structure. The NTFS file system provides more security features than the FAT system and should be used whenever security is a concern. The only reason to use FAT is for the boot partition of an ARC-compliant RISC system. A system partition using FAT can be secured in its entirety using the Secure System Partition command on the Partition menu of the Disk Administrator utility.

Among the files and directories to be protected are those that make up the operating system software itself. The standard set of permissions on system files and directories provide a reasonable degree of security without interfering with the computer's usability. For high-level security installations, you should additionally set directory permissions to all sub-directories and existing files.

The following list provides the minimum settings for C2 level file and directory ACL security as specified in the Department of Defense's "Trusted Computer System Evaluation Criteria", also known as the Orange Book:

Access Types:

Char	Dir Access	File Access
R	List Directory	Read Data
W	Add File	Write Data
X	Traverse Directory	Execute File
D	Delete	Delete
P	Change Permissions	Change Permissions
O	Take Ownership	Take Ownership
None	No Access	No Access
All	RWXDPO	RWXDPO

Access Combination Types:

Access Name	Dir Access	File Access
Full Control	All	All
Change	RWXD	RWXD
Add & Read	RWX	RX
Read	RX	RX
Add	WX	None
List	RX	None
No Access	None	None

Directory	Permissions	
`%SystemDrive%\` *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
`%SystemDrive%\` `*.*`	Everyone: Full Control	Applied ☐

`%SystemDrive%\`
`IO.SYS`
`MSDOS.SYS`
	Administrators: Full Control
	Everyone: Change
	SYSTEM: Full Control
		Applied ☐

`%SystemDrive%\`
`BOOT.INI`
`NTDETECT.COM`
`NTLDR.`
	Administrators: Full Control
	SYSTEM: Full Control
		Applied ☐

`%SystemDrive%\`
`AUTOEXEC.BAT`
`CONFIG.SYS`
	Administrators: Full Control
	Everyone: Read
	SYSTEM: Full Control
		Applied ☐

`%SystemDrive%\TEMP\` *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
`%SystemDrive%\USERS\` *(and subdirectories)*	Administrators: RWXD Everyone: List SYSTEM: Full Control	Applied ☐

%SystemDrive%\USERS\ DEFAULT\ *(and subdirectories)*	CREATOR OWNER: Full Control Everyone: RWX SYSTEM: Full Control	Applied ☐
%SystemDrive%\WIN32APP\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\ *.*	Administrators: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\ *.INI	Administrators: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\ LOCALMON.DLL PRINTMAN.HLP	Administrators: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\REPAIR *(and subdirectories)*	Administrators: Full Control	Applied ☐
%SystemRoot%\SYSTEM\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ AUTOEXEC.NT CMOS.RAM CONFIG.NT MIDIMAP.CFG	Administrators: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ PASSPORT.MID	Everyone: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ CONFIG\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ CONFIG\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: List SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ CONFIG\ SAM. SAM.LOG SECURITY. SECURITY.LOG SYSTEM. SYSTEM.ALT SYSTEM.LOG	Everyone: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ CONFIG\ USERDEF.	Administrators: Full Control Everyone: Read SYSTEM: Change	Applied ☐

%SystemRoot%\SYSTEM32\ DHCP\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ DRIVERS\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ OS2\ OSO001.009	Administrators: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ OS2\ DLL\ DOSCALLS.DLL	Administrators: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ OS2\ DLL\ NETAPI.DLL	Everyone: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ RAS\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ RAS\ *.*	Administrators: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ EXPORT\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ EXPORT\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ EXPORT\ SCRIPTS\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ EXPORT\ SCRIPTS\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ IMPORT\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ IMPORT\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Change SYSTEM: Full Control	Applied ☐

%SystemRoot%\SYSTEM32\ REPL\ IMPORT\ SCRIPTS\	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ REPL\ IMPORT\ SCRIPTS\ *.*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ SPOOL\ *(and subdirectories)*	Administrators: Full Control CREATOR OWNER: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ SPOOL\ DRIVERS\ W32X86\ 1\	Everyone: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ SPOOL\ PRTPROCS\ W32X86\ WINPRINT.DLL	Administrators: Full Control Everyone: Read Power Users: Change SYSTEM: Full Control	Applied ☐
%SystemRoot%\SYSTEM32\ WINS\ *(and subdirectories)*	Everyone: Full Control	Applied ☐

Information

For enhanced security superceding the C2 specification, change security settings designated for the "Everyone" group to the "Authenticated Users" group.

It is also highly advisable that Administrators manually scan the permissions on other partitions on the system and ensure that they are appropriately secured for various user accesses in their environment.

When you install Microsoft Office97 or any of its individual components (Word97. Excel97, etc.), you must be careful of how your security settings have effected Office97 related files and their ability to function properly. Failure to comply with the applications needs will result in erratic behavior including slowness, hanging and crashing.

Information

Refer to Knowledge Base Article ID: Q169387 for more details on NTFS with Office97.

Secure the Security Account Manager Database

Completed ☐

Not applicable ☐

Not implemented ☐

The Windows NT Server 4.0 System Key Hot-Fix (included in Service Pack 3) provides the capability to use strong encryption techniques to increase protection of account password information stored in the Registry by the Security Account Manager (SAM). Windows NT Server stores user account information, including a derivative of the user account password, in a secure portion of the Registry protected by access control and an obfuscation function. The account information in the Registry is only accessible to members of the Administrators group. Windows NT Server, like other operating systems, allows privileged users who are administrators access to all resources in the system. For installations that want enhanced security, strong encryption of account password derivative information provides an additional level of security to prevent administrators from intentionally or unintentionally accessing password derivatives using Registry programming interfaces.

Caution

Once you enable System Key encryption, you can not decrypt it.

The strong encryption capability with the Windows NT 4.0 System Key Hot-Fix is an optional feature. Administrators may choose to implement strong encryption by defining a System Key for Windows NT. Strong encryption protects private account information by encrypting the password data using a 128-bit cryptographically random key, known as a password encryption key. Only the private password information is strongly encrypted in the database, not the entire account database. Every system using the strong encryption option will have a unique password encryption key. The password encryption key is itself encrypted with a System Key. Strong password encryption may be used on both Windows NT Server and Workstation where account information is stored. Using strong encryption of account passwords adds additional protection for the contents of the SAM portion of the registry and subsequent backup copies of the registry information in the %SystemRoot%\REPAIR directory created using the RDISK command and on system backup tapes.

The System Key is defined using the command Syskey.exe. Only members of the Administrators group can run the Syskey.exe command. The utility is used to initialize or change the System Key. The System Key is the "master key" used to protect the password encryption key and therefore protection of the System Key is a critical system security operation.

There are three options for managing the System Key designed to meet the needs of different Windows NT environments. The System Key options are the following:

- Use a machine generated random key as the System Key and store the key on the local system using a complex obfuscation algorithm. This option provides strong encryption of password information in the registry and allows for unattended system restart.
- Use a machine generated random key and store the key on a floppy disk. The floppy disk with the System Key is required for the system to start and must be inserted when prompted after Windows NT begins the startup sequence, but before the system is available for users to logon. The System Key is not stored anywhere on the local system.
- Use a password chosen by the Administrator to derive the System Key. Windows NT will prompt for the System Key password when the system is in the initial startup sequence, but before the system is available for users to logon. The System Key password is not stored anywhere on the system. An MD5 digest of the password is used as the master key to protect the password encryption key.

The System Key options either using a password or requiring a floppy disk introduce a new prompt during the initialization of the Windows NT operating system. They offer the strongest protection option available because master key material is not stored on the system and control of the key can be restricted to a few individuals. On the other hand, knowledge of the System Key password, or possession of the System Key disk is required to boot the system. (If the System Key is saved to a floppy disk, backup copies of the System Key disk are recommended.) Unattended system restart may require that System Key material be available to the system without Administrator response. Storing the System Key on the local system using a complex obfuscation algorithm makes the key available only to core operating system security components. In the future, it will be possible to configure the System Key to obtain the key material from tamper proof hardware components for maximum security.

Caution ***If the System Key password is forgotten or the System Key floppy disk is lost, it may not be possible to start the system.***

Protect and store the System Key information safely with backup copies in the event of emergency. The only way to recover the system if the System Key is lost is using a repair disk to restore the registry to a state prior to enabling strong encryption.

Strong encryption may be configured independently on the Primary and each Backup Domain Controllers (DC). Each domain controller will have a unique password encryption key and a unique System Key. For example, the Primary DC may be configured to use a machine generated System Key stored on a disk, and Backup DC's may each use a different machine generated System Key stored on the local system. A machine generated System Key stored locally on a Primary domain controller is not replicated.

Before enabling strong encryption for Primary domain controllers, you should ensure a complete updated Backup domain controller is available to use as a backup system until changes to the Primary domain are complete and verified. Before enabling strong encryption on any system, Microsoft recommends making a fresh copy of the Emergency Repair Disk, including the security information in the registry, using the command, RDISK /S.

Information ***Refer to Knowledge Base Article ID: Q122857 for more details on using RDISK.***

The SYSKEY command is used to select the System Key option and generate the initial key value. The key value may be either a machine generated key or a password derived key. The SYSKEY command first displays a dialog showing whether strong encryption is enabled or disabled. After the strong encryption capability is enabled, it cannot be disabled. To enable strong authentication of the account database, select the option "Encryption Enabled", and click OK. A confirm dialog appears reminding the administrator to make an updated emergency repair disk. A new dialog appears presenting options for the Account Database Key. Use the options available on Account Database Key dialog to select the System Key.

After selecting the System Key option, Windows NT must be restarted for the System Key option to take effect. When the system restarts, the administrator may be prompted to enter the System Key, depending on the key option chosen. Windows NT detects the first use of the System Key and generates a new random password encryption key. The password encryption key is protected with the System Key, and then all account password information is strongly encrypted.

The SYSKEY command needs to be run on each system where strong encryption of the account password information is required. SYSKEY supports a "-l" (lower-case "L") command option to generate the master key and store the key locally on the system. This option enables strong password encryption in the registry and allows the command to run without an interactive dialog. The SYSKEY command can be used at a later time to change the System Key options from one method to another, or to change the System Key to a new key. Changing the System Key requires knowledge of, or possession of, the current System Key. If the password derived System Key option is used, SYSKEY does not enforce a minimum password length, however long passwords (greater than 12 characters) are recommended. The maximum System Key password length is 128 characters.

Information ***Refer to Knowledge Base Article ID: Q143475 for more details.***

Secure Client/Server Communications

Completed	☐
Not applicable	☐
Not implemented	☐

Service Pack 3 includes an updated version of the Server Message Block (SMB) authentication protocol, also known as the Common Internet File System (CIFS) file sharing protocol. The updated protocol has two main improvements: it supports mutual authentication, which closes a "man-in-the- middle" attack, and it supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital security signature into each SMB, which is then verified by both the client and the server.

In order to use SMB signing, you must either enable it or require it on both the client and the server. If SMB signing is enabled on a server, then clients that are also enabled for SMB signing will use the new protocol during all subsequent sessions and clients that are not enabled for SMB signing will use the older SMB protocol. If SMB signing is required on a server, then a client will not be able to establish a session unless it is enabled for SMB signing. SMB signing is disabled by default on a server system when you install the Service Pack; it is enabled by default on a workstation system when you apply the Service Pack.

These are provided by incorporating message signing into SMB packets that are verified by both server and client ends. There are Registry key settings to enable SMB signatures on each side. To ensure that SMB server responds to clients with message signing only, configure the following key values:

Information

These settings are useful only in a pure NT environment, as they are not supported by legacy Windows 3.1x or 95 systems.

NT Server:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value	EnableSecuritySignature
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value	RequireSecuritySignature
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

NT Workstation:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\Rdr\Parameters
Value	EnableSecuritySignature
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\Rdr\Parameters
Value	RequireSecuritySignature
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Using SMB signing will slow down the systems performance when enabled. This setting should only to be used when network security is a major concern. Performance decrease usually averages between 10 to 15%. The very nature of SMB signing requires that every packet is signed for and every packet must be verified.

Information

Refer to Knowledge Base Article ID: Q161372 for more details.

Secure Event Log Viewing

Administrators can restrict remote access to the System and Application Log files by defining a registry entry to configure whether the Event Log Service permits the "Anonymous" user to access log files. The Event Log Service does not allow the "Anonymous" user access to the Security log information. Restricting the System and Application log information from the "Anonymous" user is controlled by defining the following Registry value.

This value must be defined on each of the Event Log files. You should also alter the permission on the key to prevent unauthorized users from disabling the key's functionality.

Completed ☐

Not applicable ☐

Not implemented ☐

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\EventLog\<LogName>
Value	RestrictGuestAccess
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Secure Performance Data

Windows NT provides access to a variety of performance data that collectively represents the state of the computer. This performance data is stored in the Registry key HKEY_PERFORMANCE_DATA. The default configuration of Windows NT gives everyone the ability to query this performance data, including remote users.

In some environments, you should restrict access to this performance data because some performance data may be considered sensitive. An example of potentially sensitive performance data is the list of running processes in the system. This article describes how to regulate access to this performance data programmatically by using the Win32 API.

Completed ☐

Not applicable ☐

Not implemented ☐

The security settings on the Registry key dictate which users or groups can gain access to the performance data.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib

⚠ Information

Refer to Knowledge Base Article ID: Q146906 for more details.

Secure Print Driver Installation

This Registry key will allow you to restrict who can add printer drivers to the system. This may or may not be necessary depending on if you need to restrict users from adding their own printers. Generally, printer security restrictions are applied where the printer is being shared to prevent network users from creating a network printer.

- On NT Server, printer installations will be restricted to Administrators and Print Operators.
- On NT Workstation, printer installations will be restricted to Power Users.

Completed ☐

Not applicable ☐

Not implemented ☐

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentcontrolSet\Control\Print\Providers\LanMan Print Services\Servers
Value	AddPrintDrivers
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Secure Services for an Internet or Firewall Server

With the increased vulnerability of an NT system that is exposed directly to the Internet, it is extremely important to minimize the services that are in use and available to attack.

Completed ☐

Not applicable ☐

Not implemented ☐

For an Internet or Firewall server the actual services necessary for operation are limited. By removing or disabling any and all services that are not required, you greatly decrease the likely-hood of falling pray to a currently known or future exploitation of those services.

A large percentage of vulnerability stems from the Server and Workstation services. Therefore if applicable in your situation, they should be stopped. After the Workstation and Server services are stopped, you will not be able to perform most administrative functions. You should install these services and then disable them before the system is used in a production environment. Some applications may require the Server or Workstation services to run properly. In this case, you will also have to have a transport mechanism for the service. This transport mechanism should be a non-routable protocol such as NetBIOS. The importance of it being a non-routing protocol is so the system will be less susceptible to internet-type attacks that would be allowed access via a routing protocol such as TCP/IP.

You should disable Server and Workstation services for the MOST secure firewall implementation. If it is required that your firewall participate in your NT domain, then disable WINS bindings on the network interface that is the "outside" of the firewall. Enable only WINS bindings for the Server and Workstation services on the interface for the "inside" of the firewall (that is directly connected to your NT Domain LAN. This will minimize the chances of compromising a secure server due to Microsoft specific vulnerabilities on the outside interfaces only. Security issues within the firewall are discussed throughout the document.

These measures are by no means absolute in halting intrusion, but they do significantly decrease the possible avenues of attack. The next most important step at this point is to prevent any potential intruder from simulating local connectivity to the host by using utilities that will communicate via Named Pipes or other resident NT protocols over a TCP/IP Internet connection.

The following services should **not** be started:

Service	
Alerter	Removed ☐
ClipBook Server	Removed ☐
Computer Browser	Removed ☐
DHCP Client	Removed ☐
Directory Replicator	Removed ☐
Messenger	Removed ☐
Net Logon	Removed ☐
Network DDE	Removed ☐
Network DDE DSDM	Removed ☐
Plug and Play	Removed ☐
Remote Procedure Call (RPC) Locator	Removed ☐
Server*	Removed ☐
SNMP Trap Service	Removed ☐
Spooler *(only print spooling is required)*	Removed ☐
TCPIP NetBIOS Helper*	Removed ☐
Telephony Service	Removed ☐
Workstation*	Removed ☐

The following services **must** be started:

EventLog	Installed ☐
FTP Publishing Service *(for a FTP server only)*	Installed ☐
Gopher Publishing Service *(for a Gopher server only)*	Installed ☐
NT LM Security Support Provider	Installed ☐
Remote Procedure Call (RPC) Service	Installed ☐
SNMP *(only if using SNMP management)*	Installed ☐
World Wide Web Publishing Service *(for WWW server only)*	Installed ☐

The following services **may** be started if needed:

Schedule	Installed ☐
UPS	Installed ☐

⚠ Caution

Service names marked with a "*" may be required by your firewall apparatus. Failure to keep the services running may cause your firewall to fail. Consult your firewall user manual or the manufacturer for its proper configuration.

Secure Unnecessary Network Bindings

Completed ☐

Not applicable ☐

Not implemented ☐

The ability to individually bind protocol drivers, services and network adapters is an essential element in controlling specific types of access to a particular system. Its significance is most apparent in regards to a server that has dual connectivity to the internet and to an internal network, such as an Internet or firewall server.

Using the Bindings tab in the Network control panel will allow you to control (bind or unbind) which protocols and services have connectivity to the installed network cards of the system. This is a key procedure in configuring a networked Internet or firewall server because while allowing full protocol suite functionality on the internal (internal network side) network card, you can unbind and effectively disable protocol capabilities on your external (Internet side) network card that would have allowed avenues of penetration by unwanted guests. I.e., for a web server you can have the Server service bound to the private network card to allow user to post or modify html pages or graphics, while having the Server service unbound from the Internet connected network card thereby preventing external connections access to the same functionality.

For an adapter that has direct connectivity to the internet (without a firewall apparatus in-between) you should disable the following bindings from the WINS Client (TCP/IP) protocol listing:

- NetBIOS Interface
- Server
- Workstation

A Windows NT system that requires NetBIOS to be bound to an Internet side network card (for whatever reason) has two scenario options in order to maintain network security:

1. Remove the bindings between NetBIOS and WINS Client (TCP/IP). The native file sharing services (via the Server and Workstation services) will no longer be available to TCP/IP and therefore the Internet. In order to maintain operability with these servers while maintaining TCP/IP exclusion, a non-routable protocol will be necessary as a transport, such as NetBEUI.

2. Connect the NT system to the Internet on the external side of the network firewall. You can maintain network security by configuring the firewall to block ports 135, 137, 138 and 139 on both the TCP and UDP protocols. This will prevent NetBIOS traffic from passing through the firewall and into the internal network.

To block NetBIOS at the firewall, disable the following ports:

- netbios-ns 137tcp NETBIOS Name Service
- netbios-ns 137udp NETBIOS Name Service
- netbios-dgm 138tcp NETBIOS Datagram Service
- netbios-dgm 138udp NETBIOS Datagram Service
- netbios-ssn 139tcp NETBIOS Session Service
- netbios-ssn 139udp NETBIOS Session Service

If you choose to leave the Server service bound to an Internet connected network card, not only are you leaving an avenue for entry open, but you are also subjecting that server to additional concurrent connections as allowed per your licensing agreement and as predefined within the License Manager.

Restrict Access to the Schedule Service

Microsoft believes that it is allowing you greater flexibility to allow not only Administrators to modify the Schedule service, but to allow Server Operators to do so as well.

This enhancement as with any practice of loosening security on features that are exploitable is unadvisable. It is suggested that you add this Registry value, but you set its data to disable the feature. After doing so, modify the permissions to allow only Administrator to prevent anyone from enabling the feature.

Completed ☐

Not applicable ☐

Not implemented ☐

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	Submit Control
Type	REG_DWORD
Data	0 (1=enable, 0=disable)

Restrict Anonymous Network Access

Windows NT version 4.0 Service Pack 3 includes a security enhancement that restricts anonymous (null session) logons when they connect to specific named pipes including the one for the Registry.

This Registry key defines the list of named pipes that are "exempt" from this restriction.

List of pipes that the client is allowed to access by using the null session. If a pipe is not on this list, the request to access it will be denied.

Completed ☐

Not applicable ☐

Not implemented ☐

Restrict Null Access from Clients:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value	RestrictNullSessionAccess
Type	REG_DWORD
Data	True

Allowed Null Pipes:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value	NullSessionPipes
Type	REG_MULTI_SZ
Data	(add or remove names from the list as required)

Allowed Null Shares:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
Value	NullSessionShares
Type	REG_MULTI_SZ
Data	(add or remove names from the list as required)

Restrict Anonymous Network Access from Listing Account Names and Network Shares

Completed ☐

Not applicable ☐

Not implemented ☐

Windows NT has a feature where anonymous logon users can list domain user names and enumerate share names. Customers who want enhanced security have requested the ability to optionally restrict this functionality. Windows NT 4.0 Service Pack provides a mechanism for administrators to restrict the ability for anonymous logon users (also known as NULL session connections) to list account names and enumerate share names. Listing account names from Domain Controllers is required by the Windows NT ACL editor, for example, to obtain the list of users and groups to select who a user wants to grant access rights. Listing account names is also used by Windows NT Explorer to select from list of users and groups to grant access to a share.

There are similar situations where obtaining account names using an anonymous connection allows the user interface tools, including Windows NT Explorer, User Manager, and ACL editor, to administer and manage access control information across multiple Windows NT domains. Another example is using User Manager in the resource domain to add users from the trusted account domain to a local group. One way to add the account domain user to a local group in the resource domain is to manually enter a known domain\username to add access without getting the complete list of names from the account domain. Another approach is to logon to the system in the resource domain using an account in the trusted account domain.

Windows NT environments that want to restrict anonymous connections from listing account names can control this operation after installing Windows NT 4.0 Service Pack 3. Administrators who want to require only authenticated users to list account names, and exclude anonymous connections from doing so, need to make the following change to the registry.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	RestrictAnonymous
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

It should be noted that even with the value of RestrictAnonymous set to 1, although the user interface tools with the system will not list account names, there are Win32 programming interfaces to support individual name lookup that do not restrict anonymous connections.

Information

Refer to Knowledge Base Article ID: Q143474 for more details.

Restrict Default Access Controls on Registry Keys

Completed ☐

Not applicable ☐

Not implemented ☐

A user with a valid user name and domain name, who also has the right to log on locally to a Windows NT computer, can have the system run a program on the local computer in a heightened security context. NOTE: The Guest account does not have access to modify the registry. By default, Windows NT domain controllers only permit administrators to log on and therefore are not vulnerable.

When a properly authenticated user logs on locally to a Windows NT computer, that user becomes a member of the "Everyone" group. The default permission on the keys cited below allow members of the "Everyone" group special access, which includes the right to Set Values or Create Subkeys. This allows members of the "Everyone" group to create an entry under the Run and RunOnce keys that contains the name of a program to run when the computer starts. The Uninstall key defines the programs to run when you remove an application. Resetting the permissions for the following three Registry Subkeys to READ resolves this issue.

Root Key	HKEY_LOCAL_MACHINE
Subkey	SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Root Key	HKEY_LOCAL_MACHINE
Subkey	SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Root Key	HKEY_LOCAL_MACHINE
Subkey	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

Information

Refer to Knowledge Base Article ID: Q126713 for more details.

Restrict Client-Side LanManager Password Authentication

Completed ☐

Not applicable ☐

Not implemented ☐

Windows NT supports the following two types of challenge/response authentication:

- LanManager (LM) challenge/response (for older Microsoft networks)
- Windows NT challenge/response (for new NT networks, 3.51 and up)

To allow access to servers that only support LM authentication, Windows NT clients currently send both authentication types. Microsoft developed a patch that allows clients to be configured to send only Windows NT authentication. This setting will only prevent a client from sending a weaker LM authentication. This will not prevent a server from accepting it. The value must be applied to all NT clients. Because of these restrictions, it is only of use in a pure NT environment.

Caution

If a Windows NT client selects level 2, it cannot connect to servers that support only LM authentication, such as Windows 95 and Windows for Workgroups.

Valid range for authentication types:

- Level 0 : Send LM and Windows NT authentication (default).
- Level 1 : Send Windows NT authentication and LM authentication only if the server requests it.
- Level 2 : Never send LM authentication.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	LMCompatibilityLevel
Type	REG_DWORD
Data	2 (0=both, 1=request, 2=never)

Information

Refer to Knowledge Base Article ID: Q147706 for more details.

Auditing

Windows NT includes auditing features you can use to collect information about how your system is being used. These features also allow you to monitor events related to system security, to identify any security breaches, and to determine the extent and location of any damage. The level of audited events is adjustable to suit the needs of your organization. Some organizations need little auditing information, whereas others would be willing to trade some performance and disk space for detailed information they could use to analyze their system.

Information

Remember that when you enable auditing, there is a small performance overhead for each audit check the system performs.

Windows NT can track events related to the operating system itself and to individual applications. Each application can define its own audit-able events. Definitions of these events are added to the Registry when the application is installed on your Windows NT computer. Audit events are identified to the system by the event source module name (which corresponds to a specific event type in the Registry) and an event ID. In addition to listing events by event ID, the security log in Event Viewer lists them by category. The following categories of events are displayed in the Security Log. (Those in parentheses are found in the Audit Policy dialog box of User Manager.)

Category	***Description***
Account Management *(User and Group Management)*	These events describe high-level changes to the user accounts database, such as User Created or Group Membership Change. Potentially, a more detailed, object-level audit is also performed (see Object Access events).
Detailed Tracking *(Process Tracking)*	These events provide detailed subject-tracking information. This includes information such as program activation, handle duplication, and indirect object access.
Logon/Logoff *(Logon and Logoff)*	These events describe a single logon or logoff attempt, whether successful or unsuccessful. Included in each logon description is an indication of what type of logon was requested or performed (that is, interactive, network, or service).
Object Access *(File and Object Access)*	These events describe both successful and unsuccessful accesses to protected objects.
Policy Change *(Security Policy Changes)*	These events describe high-level changes to the security policy database, such as assignment of privileges or logon capabilities. Potentially, a more detailed, object-level audit is also performed (see Object Access events).
Privilege Use *(Use of User Rights)*	These events describe both successful and unsuccessful attempts to use privileges. It also includes information about when some special privileges are assigned. These special privileges are audited only at assignment time, not at time of use.
System Event *(System)*	These events indicate something affecting the security of the entire system or audit log occurred.

Use the following chart to help determine your best course of action dependant on the type of threat you wish to log events on:

Threat	***Practical Action***
Break-in using brute-force hacked passwords	Enable failure auditing for log on and log off events.
Break-in using stolen password	Enable success auditing for log on and log off events. The log entries will not distinguish between the real users and the phony ones. What you are looking for here is unusual activity on user accounts, such as logons at odd hours or on days when you would not expect any activity.
Misuse of administrative privileges by authorized users	Enable success auditing for use of user rights; for user and group management, for security policy changes; and for restart, shutdown and system events. (Note: Because of the high volume of events that would be recorded, Windows NT does not normally audit the use of the Backup Files And Directories and the Restore Files And Directories rights.

Virus outbreak	Enable success and failure write access auditing for program files such as files with .exe and .DLL extensions. Enable success and failure process tracking auditing. Run suspect programs and examine the security log for unexpected attempts to modify program files or creation of unexpected processes. Note that these auditing settings generate a large number of event records during routine system use. You should use them only when you are actively monitoring the system log.
Improper access to sensitive files	Enable success and failure auditing for file and object access events. Then use File Manager to enable success and failure auditing of read and write access by suspect users or groups for sensitive files.
Improper access to printers	Enable success and failure auditing for file and object access events. Then use Print Manager to enable success and failure auditing of print access by suspect users or groups for the printers.

Audit the System

Completed ☐
Not applicable ☐
Not implemented ☐

Enabling system auditing can inform you of actions that pose security risks and possibly detect security breaches. To activate security event logging, follow these steps:

1. Log on as the administrator of the local workstation.
2. Click the Start button, point to Programs, point to Administrative Tools, and then click User Manager.
3. On the Policies menu, click Audit.
4. Click the Audit These Events option.
5. Enable the options you want to use. The following options are available:

   - Log on/Log off (Logs both local and remote resource logins.)
   - File and Object Access (File, directory, and printer access.)
   - User and Group Management (Any account, group or passwords created, changed or deleted.)
   - Security Policy Changes (Any changes to user rights or audit policies.)
   - Restart, Shutdown, And System (Logs shutdowns and restarts for the local workstation.)
   - Process Tracking: (Tracks program activation, handle duplication, indirect object access, and process exit.)

   Click the Success check box to enable logging for successful operations, and the Failure check box to enable logging for unsuccessful operations.

6. Click OK

Information

Auditing is a detection technique rather than a form of prevention. Although it will help you discover the details of a security breach after it has occurred, you can use those details for preventing it from happening again.

Audit Base Objects

Completed ☐
Not applicable ☐
Not implemented ☐

This Registry setting tells the Local Security Authority (LSA) that base objects should be created with a default system audit control list. It does not start generating audits on all Base Objects. For existing Base Objects, the Administrator will need to turn auditing on for the "Object Access" category using the User Manager.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	AuditBaseObjects
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Audit Privileges

Completed ☐

Not applicable ☐

Not implemented ☐

Certain privileges in the system are not audited by default even when auditing on privilege use is turned on. This is done to control the growth of audit logs. The privileges are:

1. Bypass traverse checking (given to everyone).
2. Debug programs (given only to administrators)
3. Create a token object (given to no one)
4. Replace process level token (given to no one)
5. Generate Security Audits (given to no one)
6. Backup files and directories (given to administrators and backup operators)
7. Restore files and directories (given to administrators and backup operators)

1 is granted to everyone so it is meaningless from an auditing perspective. 2 is not used in a working system and can be removed from administrators group. 3, 4 and 5 are not granted to any user or group and are highly sensitive privileges and should not be granted to anyone. However 6 and 7 are used during normal system operations and are expected to be used. To enable auditing of these privileges, add the following key value to the Registry key

Caution

These privileges are not audited by default because backup and restore is a frequent operation and this privilege is checked for every file and directory backed or restored, which can lead to thousands of audits filling up the audit log in no time. Carefully consider turning on auditing on these privilege uses

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	FullPrivilegeAuditing
Type	REG_BINARY
Data	1 (1=enable, 0=disable)

Disable Automatic Administrative Shares

By default, Windows NT automatically shares what Microsoft considers to be critical areas of the OS installation. The shares are only accessible by users belonging to the Administrator group strictly for administrative purposes. Refer to Appendix [A] for more details on what volumes are shared.

Depending on the server's content, leaving the Administrative Share's active may not be a provide adequate security (i.e. financial or HR resources).

Completed ☐

Not applicable ☐

Not implemented ☐

NT Server:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Value	AutoShareServer
Type	REG_BINARY
Data	0 (1=enable, 0=disable)

NT Workstation:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
Value	AutoShareWks
Type	REG_BINARY
Data	0 (1=enable, 0=disable)

Disable Caching of Logon Credentials

Microsoft Windows NT caches previous users' logon information locally so that they will be able to log on in the event that a logon server is unavailable during subsequent logon attempts.

Through the registry and a resource kit utility (`Regkey.exe`), you are able to change the number of previous logon attempts that a server will cache. By default, Windows NT will remember the 10 most recent logon attempts. The valid range of values for this parameter is 0 to 50. A value of 0 disables logon caching and any value above 50 will only cache 50 logon attempts.

Completed ☐

Not applicable ☐

Not implemented ☐

This feature is provided for system availability reasons such as the user's machine is disconnected or none of the domain controllers are online. They can continue to work in within the same environmental parameters as their roaming profile. When disabled, the user would be forced to logon locally to the machine, and a different profile.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	CachedLogonsCount
Type	REG_SZ
Data	0 (1-50 cached logons, 0=disable)

Information

Refer to Knowledge Base Article ID: Q172931 for more details.

Disable Display of Last User Name

By default, Windows NT places the user name of the last user to log on the computer in the User name text box of the Logon dialog box. This makes it more convenient for the most frequent user to log on. To help keep user names secret, you can prevent Windows NT from displaying the user name from the last log on. This is especially important if a computer that is generally accessible is being used by the (hopefully renamed) built-in Administrator account.

To prevent display of a user name in the Logon dialog box, enable the following Registry value.

Completed ☐

Not applicable ☐

Not implemented ☐

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	DontDisplayLastUserName
Type	REG_SZ
Data	1 (1=enable, 0=disable)

Information

Refer to Knowledge Base Article ID: Q114463 for more details.

Disable Guest Account

Casual access through a guest account should not be permitted what-so-ever. A user that has logged onto a network now has Domain User privileges that can be exploited.

This "Guest User" could now launch such utilities as "GetAdmin" to gain administrative rights or "WinNuke" to flood TCP/IP ports causing networked systems to crash.

Because of the Guest accounts anonymity, you would not be able to track the culprit by auditing your security logs. It is reasons such as these that demonstrate why it is essential that all users must have valid accounts

Completed ☐

Not applicable ☐

Not implemented ☐

Disable Removable Disk Access from Network

Because the CD-ROM and Floppy drives are volumes, by default they are shared as administrative shares on the network. If the data of these entries are 1, the drives are allocated to the user as part of the interactive logon process and, therefore, only the current user can access it. This prevents network administrators and remote users (and even the same user at a different workstation) from accessing the drive while the current user is logged on. The drive is shared again when the current user logs off.

This value entry satisfies, in part, the C2 security requirement that you must be able to secure removable media.

Completed ☐

Not applicable ☐

Not implemented ☐

CD-ROMS:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	AllocateCDRoms
Type	REG_SZ
Data	1 (1=enable, 0=disable)

Floppy Diskettes:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	AllocateFloppies
Type	REG_SZ
Data	1 (1=enable, 0=disable)

Disable Shutdown Without Logon

In Windows NT Workstation, the Shutdown button is available in the Welcome screen after pressing <CTRL+ALT+DEL> to log on. However, in Windows NT Server, by default, the Shutdown button is not available. The ability to display the Shutdown button is configurable for both Workstation and Server via the Registry.

Normally, you can shut down a computer running Windows NT Workstation without logging on by choosing Shutdown in the Logon dialog box. This is appropriate where users can access the computer's operational switches; otherwise, they might tend to turn off the computer's power or reset it without properly shutting down Windows NT Workstation. However, you can remove this feature if the CPU is locked away.

Completed ☐

Not applicable ☐

Not implemented ☐

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	ShutdownWithoutLogon
Type	REG_SZ
Data	0 (1=enable, 0=disable)

Information

Refer to Knowledge Base Article ID: Q114817, Q143164 for more details.

Logging Off or Locking the System

Users should either log off or lock the system if they will be away from the computer for any length of time. Logging off allows other users to log on (useful in a computer sharing environment); locking the system does not (except by administrators).

The system can be set to lock automatically if it is not used for a set period of time by using any 32-bit screen saver with the Password Protected option.

It is recommended that a password protected screen saver is installed that automatically starts if the system is not used for minimum of 5 minutes

Completed ☐

Not applicable ☐

Not implemented ☐

Rename the Administrator Account

This, the most powerful of accounts, is the one account that can never be locked out due to repeated failed log on attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. By renaming the account, you afford yourself added protection by making it difficult for potential hackers to recognize the account.

Completed ☐
Not applicable ☐
Not implemented ☐

In order to completely secure the account from network intrusion, must modify User Rights Policy and make the following configuration changes for the Right "Access this computer from network":

- Remove the Administrators group
- Add individuals accounts for users with Administrator rights

Caution

Administrator rights should only be set for necessary administrators and only on necessary servers.

Wipe the Page File at a Clean System Shutdown

Virtual Memory support of Windows NT uses a system page file (`pagefile.sys`) to swap pages from memory of different processes onto disk when they are not being actively used. On a running system, this page file is opened exclusively by the operating system and therefore is protected from active viewing and manipulation. However, once the page file is no longer locked for exclusively use the file may be viewed, exposing the raw data from previously opened applications and system processes. This can be exploited simply by booting the system from an alternative OS, either from a bootable floppy or a multiple-boot hard disk partition. There are shareware utilities such as NTFS File System Driver for DOS/Windows by Mark Russinovich and Bryce Cogswell, that will allow NTFS partition reading from a MS-DOS FAT booted floppy in the shareware version. The full commercial product will allow you to write to NTFS as well.

Completed ☐
Not applicable ☐
Not implemented ☐

This problem is even more critical in a mixed Novell NetWare environment because Microsoft's Client Services for NetWare and Novell's IntranetWare Client for Windows NT write plain-text user-ID's and password information to the page file. Although this password security risk only applies to NetWare, users will typically use the same password for both systems, thereby escalating the need to secure this even further. Clearing the page file at shutdown helps eliminate this problem.

Caution

This protection works only during a clean shutdown. Therefore, it is important that non-trusted users do not have ability to power off or reset the system manually.

If this security feature is enabled, when the system shuts down Windows NT will attempt to fill all inactive pages in the page file with zeros so that there will be no data when the file is no longer exclusively locked. However, it cannot fill active pages with zeros because they are being used by the system or other remaining active processes

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Session Manager \Memory Management
Value	ClearPageFileAtShutdown
Type	REG_DWORD
Data	1 (1=enable, 0=disable)

Customize the Logon

Completed ☐

Not applicable ☐

Not implemented ☐

Because the logon dialog box Windows NT displays can be interpreted as an invitation to enter your network (whether as a valid user or otherwise), it is important to begin the legalities of the user's actions, starting at the logon prompt.

First and foremost you should implement a legal notice that will display prior to the user being able to logon. It will require that they click "ok" to continue through, but this should prove to be of little consequence as the average user only logs on once per day.

Second, customize the logon prompt itself with a welcome greeting and brief instructions on how to enter their name and password. Not only does this remind them that they are indeed in a place of work and they are actually logging on/entering commercial property, but it can be used as a friendly greeting to break the monotonous staleness of the computer environment that they are in.

Legal Notice Caption:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	LegalNoticeCaption
Type	REG_SZ
Data	<variable text>

Legal Notice Message Text:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	LegalNoticeText
Type	REG_SZ
Data	<variable text>

Logon Prompt:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	LogonPrompt
Type	REG_SZ
Data	<variable text>

Welcome Message:

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Value	Welcome
Type	REG_SZ
Data	<variable text>

Enforce Strong User Passwords

Completed ☐

Not applicable ☐

Not implemented ☐

Windows NT 4.0 Service Pack 2 (and later) includes a new DLL file (Passfilt.dll) that lets you enforce stronger password requirements for users. Passfilt.dll provides enhanced security against "password guessing" or "dictionary attacks" by outside intruders.

Passfilt.dll implements the following password policy:

1. Passwords must be at least six (6) characters long.
2. Passwords must contain characters from at least three (3) of the following four (4) classes:

Description	***Examples***
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters") such as punctuation symbols	

3. Passwords may not contain your user name or any part of your full name.

These requirements are hard-coded in the Passfilt.dll file and cannot be changed through the user interface or Registry. If you wish to raise or lower these requirements, you may write your own .DLL and implement it in the same fashion as the Microsoft version that is available with Windows NT 4.0 Service Pack 2 (or later).

To ensure that Strong Password functionality occurs throughout your domain structure, make the necessary Registry changes on all PDC's. It is suggested that you do the same to all BDC's as well, in case of a server role change necessitated by want or need.

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SYSTEM\CurrentControlSet\Control\Lsa
Value	Notification Packages
Type	REG_MULTI_SZ
Data	PASSFILT

Information

Refer to Knowledge Base Article ID: Q151082, Q161990 for more details.

Internet Usage and Security Policy Template

This template is meant only to give you guidance in creating a policy for your particular organization's needs. The following suggestions may have little or no bearing to your organization's current policy. Some of the suggestions may even be prohibited by law within your local jurisdiction. It is important that you review this template carefully before implementing any of these policies. As with any organization-wide policy, it should be verified to fit your organization's needs and thoroughly checked by a competent attorney who is familiar with those needs.

Policy Overview

This company provides access to the vast information resources of the Internet to help you do your job faster and smarter, and be a well-informed business citizen. The facilities to provide that access represent a considerable of company resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While we have set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost, the Internet for this company is a business tool provided to you at significant cost. That means we expect you to use your internet access [*primarily*] for business-related purposes, i.e., to communicate with customers and suppliers, to research relevant topics and obtain useful business information [*except as outlined below*]. We insist that you conduct honestly and appropriately on the Internet, and respect the copyrights, software-licensing rules, property rights, privacy prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing company policies apply to your conduct on the internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the company and expose the firm to significant liabilities.

The chats, newsgroups and email of the Internet give each individual Internet user and immense and unprecedented reach to propagate company messages and tell our business story. Because of that power, we must take special care to maintain the clarity, consistency and integrity of the company's corporate image and posture. Anything any one employee writes in the course of acting for the company on the Internet can be taken as representing the company's corporate posture. That is why we expect you to forego a measure of your individual freedom when you participate in chats or newsgroups on company business, as outlines below.

While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principal is that security is to be everyone's first concern. An Internet use can be held accountable for any breaches of security or confidentiality.

Certain terms in this policy should be understood expansively to include related concepts. **Company** includes our affiliates, subsidiaries and branches. **Document** covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. **Graphics** include photographs, pictures, animations, movies or drawings. **Display** includes monitors, flat-panel active or passive matrix displays, monochrome LCD's, projectors, televisions and virtual-reality tools.

All employees granted Internet access with company facilities will be provided with a written copy of this policy. All Internet users must sign the following statement:

> "I have received a written copy of my company's Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may record for management use the internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to dismissal or even criminal prosecution."

Detailed Internet Policy Provisions

Management and Administration

1. The company has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems are capable of recording (for each and every user) each World Wide Web site visit, chat, newsgroups or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our managers will review Internet activity and analyze usage patterns, and they may choose to publicize the data to assure that company Internet resources are devoted to maintaining the highest levels of productivity.
2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
3. The display of any sexually explicit image or document on any company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded our network or computing resources.
4. The company uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.
5. The company's facility and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any company resources for illegal activity is ground for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
6. Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with the licenses or copyrights.
7. No employee may use company facilities knowingly to download or distribute pirated software or data.
8. No employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code.
9. No employee may use the company's Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
10. Each employee using the internet facilities of the company shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.
11. Only those employees or officials who duly authorized to speak to the media, to analysts or in public gatherings on behalf of the company may speak/write in the name of the company to any newsgroup or chat room. Other employee may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this company, the employee must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the company of any commercial product or service not sold or serviced by this company, its subsidiaries or its affiliates. Only those manager and company officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the company may grant such authority to newsgroups or chat room participants.
12. The company retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

13. Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures. Employees releasing protected information via newsgroup or chat (whether or not the release in inadvertent) will be subject to all penalties under existing data security policies and procedures.
14. Use of company internet access facilities to commit infractions such as misuse of company assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited by general company policy, and will be sanctioned under the relevant provisions of the personnel handbook.

Technical

1. User ID's and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource must keep the password confidential. Company policy prohibits the sharing of user ID's or passwords obtained for access to Internet sites.
2. Employee's should schedule communications-intensive operations such as large file transfers, video downloads, mass emailing and the like for off-peak times (defined however that is appropriate for the particular company).
3. Any file that is downloaded must be scanned for viruses before it is run or accessed.

Security

1. The company has installed [*a variety of firewalls, proxies, Internet address screening programs and other security systems*] to assure the safety and security of the company's networks. Any employee who attempts to disable, defeat or circumvent any company security facility will be subject to immediate dismissal.
2. Files [*containing sensitive company data as defined by existing corporate data security policy*] that are transferred in any way across the Internet must be encrypted.
3. Computers that use their own modems to create independent data connections sidestep our network security mechanisms. An individual computer's private connection to any outside computer can be used by an attacker to compromise any company network to which that computer is attached. That is why any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from company's internal networks. (Major online services such as CompuServe and America OnLine, and content providers such as Lexis-Nexis, can be accessed via firewall-protected internet connections, making insecure direct dial-up connections generally unnecessary.)
4. Only those Internet service and functions with documented business purposes for this company will be enabled at the Internet firewall.

THE REFERENCE APPENDIX

[A] Default NT Settings

The following should be used to demonstrate why it is imperative to systematically alter the Access Control List (ACL) file and directory permissions throughout the NT Installation of both Server and Workstation systems.

Directory ACL Permissions

Directory	*Type*	*User Groups*
\ (Root)	Full Control	Administrators
	Change	Server Operators, Everyone
%SystemRoot%	Full Control	Administrators, Creator/Owner
	Change	Server Operators, Everyone
%SystemRoot%\Config	Full Control	Everyone
%SystemRoot%\Profiles	Full Control	Everyone
%SystemRoot%\Profiles\All Users	Full Control	Administrators
	Read	Everyone
%SystemRoot%\System	Full Control	Administrators, Creator/Owner
	Change	Server Operators, Everyone
%SystemRoot%\System32	Full Control	Administrators, Creator/Owner
	Change	Server Operators, Everyone
\Win32App	Full Control	Administrators, Server Operators, Creator/Owners
\Program Files	Full Control	Everyone
\Temp	Full Control	Administrators, Creator/Owner
	Change	Server Operators, Everyone
\Users	Special	Administrators, Account Operators
	Read	Everyone

Hidden Network Shares

Share Name	*Function*	*Through*	*User Groups*
x$	Remote administrative share to entire disk volume, also known as %SystemDrive%	Full Control	Administrators, Server Operators, Backup Operators
Admin$	Remote administrative share to the NT installation directory, also known as %SystemRoot%	Full Control	Administrators, Server Operators, Backup Operators
IPC$	Remote administrative share used for named-pipes support		Everyone
Print$	Resource for printer sharing	Full Control	Administrators, Power Users
		Read	Everyone
Repl$	Resource for NTS replication partners	Full Control	Administrators
		Read	Replicator

Open Service Ports

Windows NT Functionality	*UDP*	*TCP*	*IP*
Browsing	137,138		
DHCP Lease	67,68		
DHCP Manager		135	
DNS Administration		139	
DNS Resolution	53		
File Sharing		139	
Logon Sequence	137,138	139	
NetLogon	138		
NT Diagnostics		139	
NT Directory Replication	138	139	
NT Event Viewer		139	
NT Performance Monitor		139	
NT Registry Editor		139	
NT Secure Channel	137,138	139	
NT Server Manager		139	
NT Trusts	137,138	139	
NT User Manager		139	
Pass Through Validation	137,138	139	
PPTP		1723	47
Printing	137,138	139	
WINS Manager		135	
WINS Registration		137	
WINS Replication		42	

Exchange Functionality			
Client/Server Comm.		135	
Exchange Administrator		135	
IMAP		143	
LDAP		389	
LDAP (SSL)		636	
MTA - X.400 over TCP/IP		102	
POP3		110	
RPC		135	
SMTP		25	

[B] Software Installation Subkey Locations

Hot-Fixes

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix

Outlook/Exchange Client Extensions

Root Key	HKEY_LOCAL_MACHINE
Subkey	\SOFTWARE\Microsoft\Exchange\Client\Extensions

[C] C2 and the Trusted Computer System Evaluation Criteria

The National Computer Security Center (NCSC) is the United States government agency responsible for performing software product security evaluations. These evaluations are carried out against a set of requirements outlined in the NCSC publication "Department of Defense Trusted Computer System Evaluation Criteria", which is commonly referred to as the “Orange Book.”

Windows NT has been successfully evaluated by the NCSC at the C2 security level as defined in the Orange Book, which covers the base operating system.

Information

Windows NT in its COTS state does not comply to the C2 specification.

You must configure NT to be secure, as outlined partly in this document and in the "Department of Defense Trusted Computer System Evaluation Criteria" specification.

Because the C2 standard only involves the base operating system, a C2 compliant system may not participate in a network environment. It must remain isolated. Windows NT has not yet been evaluated by the NCSC "Trusted Network Interpretation" specification, commonly referred to as the "Red Book", which would give it a networking security rating.

Trusted Computer System Evaluation Criteria Classes

Class (D): Minimal Protection

This class is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Class (C1): Discretionary Security Protection

The Trusted Computing Base (TCB) of a class C1 system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class C1 environment is expected to be one of cooperating users processing data at the same level(s) of sensitivity.

Class (C2): Controlled Access Protection

Systems in this class enforce a more finely grained discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Class (B1): Labeled Security Protection

Class B1 systems require all the features required for class C2. In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. Any flaws identified by testing must be removed.

Class (B2): Structured Protection

In class B2 systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class B1 systems be extended to all subjects and objects in the ADP system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non- protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class (B3): Security Domains

The class B3 TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to

exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security- relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Class (A1): Verified Design

Systems in class A1 are functionally equivalent to those in class B3 in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class (A1), more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

[D] NetBIOS Names

Microsoft networking services running on a Windows NT-based computer are identified by using NetBIOS names. NetBIOS names can be used to identify a unique computer or a special group of computers. NetBIOS names are 16 characters in length and the 16th character is a special character used by most Microsoft networking services. Various networking service and group names are registered with a WINS server by direct name registration from WINS-enabled computers or by broadcast on the local subnet by non-WINS enabled computers.

The nbtstat command is a utility that you can use to obtain information about NetBIOS names. In the following example, the nbtstat -n command produced this list of registered NetBIOS names for user “MESPINOLA” logged on to a computer configured as a primary domain controller and running under Windows NT Server with Internet Information Server.

Names

Name	*16TH*	*Type*	*Description*
MESPINOLA1	<00>	UNIQUE	workstation service name
MESPINOLA1	<20>	GROUP	server service name
MESPINOLAD	<00>	GROUP	domain name
MESPINOLAD	<1C>	UNIQUE	domain controller name
MESPINOLAD	<1B>	UNIQUE	master browser name
MESPINOLA1	<03>	UNIQUE	messenger name
INet~Services	<1C>	GROUP	Internet Information Server group name
IS~MESPINOLA1..	<00>	UNIQUE	Internet Information Server unique name
MESPINOLA1+++++	<BF>	UNIQUE	network monitor name

Unique-Type Names

16TH Byte	*Description*
<00>	Workstation service name. In general, this is the name that is referred to as the NetBIOS computer name.
<03>	Messenger service name used when receiving and sending messages. This is the name that is registered with the WINS server as the messenger service on the WINS client and is usually appended to the computer name and to the name of the user currently logged on to the computer.
<1B>	Domain master browser name. This name identifies the primary domain controller and indicates which clients and other browsers to use to contact the domain master browser.
<06>	RAS server service
<1F>	NetDDE service
<20>	Server service name used to provide share-points for file sharing.
<21>	RAS client
<BE>	Network Monitor agent
<BF>	Network Monitor utility

Group-Type Names

16TH Byte	*Description*
<1C>	A domain group name, which contains a list of the specific addresses of computers that have registered the domain name. The domain controller registers this name. WINS treats this as a domain group, where each member of the group must renew its name individually or be released. The domain group is limited to 25 names. When a static 1C name is replicated that clashes with a dynamic 1C name on another WINS server, a union of the members is added, and the record is marked as static. If the record is static, members of the group do not have to renew their IP addresses.
<1D>	The master browser name that is used by clients to access the master browser. There is one master browser on a subnet. WINS servers return a positive response to domain name registrations but do not store the domain name in their databases. If a computer sends a domain name query to the WINS server, the WINS server returns a negative response. If the computer that sent the domain name query is configured as h-node or m-node, it will then broadcast the name query to resolve the name.
<1E>	A Normal group name. Browsers can broadcast to this name and listen on it to elect a master browser. These broadcasts are for the local subnet and should not cross routers.
<20>	A special group name called the Internet group that is registered with WINS servers to identify groups of computers for administrative purposes. For example, “printersg” could be a registered group name used to identify an administrative group of print servers.
MSBROWSE,	Instead of a single appended 16th character, “_MSBROWSE_,” is appended to a domain name and broadcast on the local subnet to announce the domain to other master browsers.

[E] Port Assignments

In TCP/IP, a port is the mechanism that allows a computer to simultaneously support multiple communication sessions with computers and programs on the network. A port is basically a refinement of an IP address; a computer that receives a packet from the network can further refine the destination of the packet by using a unique port number that is determined when the connection is established. A number of "well known" ports have reserved numbers that correspond to predetermined functions.

This appendix describes the Windows NT Server and Windows NT Workstation default port assignments for TCP/IP and UDP. The Services file controls port assignments used by Windows NT Server and Windows NT Workstation. The Services file is located in the \systemroot\Winnt\System32\Drivers\Etc\Services directory

NT Service Port Assignments

Port	*Protocol*	*Service Name*	*Alias*	*Comment*
7	tcp, udp	echo		
9	tcp, udp	discard	sink null	
11	tcp, udp	systat	users	
13	tcp, udp	daytime		
15	tcp	netstat		
17	tcp, udp	qotd	quote	
19	tcp, udp	chargen	ttytst source	
20	tcp	ftp-data		
21	tcp	ftp		
23	tcp	telnet		
25	tcp	smtp	mail	
37	tcp, udp	time	timserver	
39	udp	rlp	resource	resource location
42	tcp, udp	name	nameserver	
43	tcp	whois	nicname	usually to sri-nic
53	tcp, udp	domain	nameserver	name-domain server
53	tcp, udp	nameserver	domain	name-domain server
57	tcp	mtp		deprecated
67	udp	bootp		boot program server
69	udp	tftp		
77	tcp	rje	netrjs	
79	tcp	finger		
87	tcp	link	ttylink	
95	tcp	supdup		
101	tcp	hostnames	hostname	usually from sri-nic
102	tcp	iso-tsap		
103	tcp	dictionary	webster	
103	tcp	x400		ISO Mail
104	tcp	x400-snd		
105	tcp	csnet-ns		
109	tcp	pop	postoffice	
109	tcp	pop2		Post Office
110	tcp	pop3	postoffice	
111	tcp, udp	portmap		
111	tcp, udp	sunrpc		
113	tcp	auth	authentication	
115	tcp	sftp		
117	tcp	path		
117	tcp	uucp-path		
119	tcp	nntp	usenet	Network News Transfer
123	udp	ntp	ntpd ntp	network time protocol (exp)

137	udp	nbname		
138	udp	nbdatagram		
139	tcp	nbsession		
144	tcp	NeWS	news	
153	udp	sgmp	sgmp	
158	tcp	tcprepo	repository	PCMAIL
161	udp	snmp	snmp	
162	udp	snmp-trap	snmp	
170	tcp	print-srv		network PostScript
175	tcp	vmnet		
315	udp	load		
400	tcp	vmnet0		
500	udp	sytek		
512	udp	biff	comsat	
512	tcp	exec		
513	tcp	login		
513	udp	who	whod	
514	tcp	shell	cmd	no passwords used
514	udp	syslog		
515	tcp	printer	spooler	line printer spooler
517	udp	talk		
518	udp	ntalk		
520	tcp	efs		for LucasFilm
520	udp	route	router routed	
525	udp	timed	timeserver	
526	tcp	tempo	newdate	
530	tcp	courier	rpc	
531	tcp	conference	chat	
531	udp	rvd-control	MIT disk	
532	tcp	netnews	readnews	
533	udp	netwall		-for emergency broadcasts
540	tcp	uucp	uucpd	uucp daemon
543	tcp	klogin		Kerberos authenticated rlogin
544	tcp	kshell	cmd	and remote shell
550	udp	new-rwho	new-who	experimental
556	tcp	remotefs	rfs_server rfs	Brunhoff remote filesystem
560	udp	rmonitor	rmonitord	experimental
561	udp	monitor		experimental
600	tcp	garcon		
601	tcp	maitrd		
602	tcp	busboy		
700	udp	acctmaster		
701	udp	acctslave		
702	udp	acct		
703	udp	acctlogin		
704	udp	acctprinter		
704	udp	elcsd		errlog
705	udp	acctinfo		
706	udp	acctslave2		
707	udp	acctdisk		
750	tcp, udp	kerberos	kdc	Kerberos authentication
751	tcp, udp	kerberos_master		Kerberos authentication
752	udp	passwd_server		Kerberos passwd server
753	udp	userreg_server		Kerberos userreg server
754	tcp	krb_prop		Kerberos slave propagation
888	tcp	erlogin		Login and environment passing

1109	tcp	kpop		Pop with Kerberos
1167	udp	phone		
1524	tcp	ingreslock		
1666	udp	maze		
2049	udp	nfs		sun nfs
2053	tcp	knetd		Kerberos de-multiplexor
2105	tcp	eklogin		Kerberos encrypted rlogin
5555	tcp	rmt	rmtd	
5556	tcp	mtb	mtbd	mtb backup
9535	tcp	man		remote man server
9536	tcp	w		
9537	tcp	mantst		remote man server, testing
10000	tcp	bnews		
10000	udp	rscs0		
10001	tcp	queue		
10001	udp	rscs1		
10002	tcp	poker		
10002	udp	rscs2		
10003	tcp	gateway		
10003	udp	rscs3		
10004	tcp	remp		
10004	udp	rscs4		
10005	udp	rscs5		
10006	udp	rscs6		
10007	udp	rscs7		
10008	udp	rscs8		
10009	udp	rscs9		
10010	udp	rscsa		
10011	udp	rscsb		
10012	tcp, udp	qmaster		

Well Known Service Port Assignments

Well known services are defined by RFC 1060. The relationship between the well known services and the well known ports is described in this excerpt from RFC 1340 (J. Reynolds and J. Postal, July 1992):

- The well known ports are controlled and assigned by the Internet Assigned Numbers Authority (IANA), and on most systems can only be used by system (or root) processes or by programs executed by privileged users.
- Ports are used in TCP to name the ends of logical connections that carry long term conversations. For the purpose of providing services to unknown callers, a service contact port is defined. This list specifies the port used by the server process as its contact port. The contact port is sometimes called the "well known port."
- UDP ports are not the same as TCP ports, though to the extent possible, TCP and UDP may use the same port assignments. The UDP specification is defined in RFC 768.
- The assigned ports use a small portion of the possible port numbers. For many years, the assigned ports were in the range 0 - 255. Recently, the range for assigned ports managed by the IANA has been expanded to the range 0 - 1023.

The following table describes both TCP and UDP port assignments for well known ports.

Port	*Protocol*	*Service Name*	*Alias*
0	tcp, udp		Reserved
1	tcp, udp	tcpmux	TCP Port Service Multiplexer
2	tcp, udp	compressnet	Management Utility
3	tcp, udp	compressnet	Compression Process
4	tcp, udp		Unassigned
5	tcp, udp	rje	Remote Job Entry
6	tcp, udp		Unassigned
7	tcp, udp	echo	Echo
8	tcp, udp		Unassigned
9	tcp, udp	discard	Discard; alias=sink null
10	tcp, udp		Unassigned
11	udp	systat	Active Users; alias=users
12	tcp, udp		Unassigned
13	tcp, udp	daytime	Daytime
14	tcp, udp		Unassigned
15	tcp, udp		Unassigned [was netstat]
16	tcp, udp		Unassigned
17	tcp, udp	qotd	Quote of the Day; alias=quote
18	tcp, udp	msp	Message Send Protocol
19	tcp, udp	chargen	Character Generator; alias=ttytst source
20	tcp, udp	ftp-data	File Transfer [Default Data]
21	tcp, udp	ftp	File Transfer [Control], connection dialog
22	tcp, udp		Unassigned
23	tcp, udp	telnet	Telnet
24	tcp, udp		Any private mail system
25	tcp, udp	smtp	Simple Mail Transfer; alias=mail
26	tcp, udp		Unassigned
27	tcp, udp	nsw-fe	NSW User System FE
28	tcp, udp		Unassigned
29	tcp, udp	msg-icp	MSG ICP
30	tcp, udp		Unassigned
31	tcp, udp	msg-auth	MSG Authentication
32	tcp, udp		Unassigned
33	tcp, udp	dsp	Display Support Protocol
34	tcp, udp		Unassigned
35	tcp, udp		Any private printer server

36	tcp, udp		Unassigned
37	tcp, udp	time	Time; alias=timeserver
38	tcp, udp		Unassigned
39	tcp, udp	rlp	Resource Location Protocol; alias=resource
40	tcp, udp		Unassigned
41	tcp, udp	graphics	Graphics
42	tcp, udp	nameserver	Host Name Server; alias=nameserver
43	tcp, udp	nicname	Who Is; alias=nicname
44	tcp, udp	mpm-flags	MPM FLAGS Protocol
45	tcp, udp	mpm	Message Processing Module
46	tcp, udp	mpm-snd	MPM [default send]
47	tcp, udp	ni-ftp	NI FTP
48	tcp, udp		Unassigned
49	tcp, udp	login	Login Host Protocol
50	tcp, udp	re-mail-ck	Remote Mail Checking Protocol
51	tcp, udp	la-maint	IMP Logical Address Maintenance
52	tcp, udp	xns-time	XNS Time Protocol
53	tcp, udp	domain	Domain Name Server
54	tcp, udp	xns-ch	XNS Clearinghouse
55	tcp, udp	isi-gl	ISI Graphics Language
56	tcp, udp	xns-auth	XNS Authentication
57	tcp, udp		Any private terminal access
58	tcp, udp	xns-mail	XNS Mail
59	tcp, udp		Any private file service
60	tcp, udp		Unassigned
61	tcp, udp	ni-mail	NI MAIL
62	tcp, udp	acas	ACA Services
63	tcp, udp	via-ftp	VIA Systems - FTP
64	tcp, udp	covia	Communications Integrator (CI)
65	tcp, udp	tacacs-ds	TACACS-Database Service
66	tcp, udp	sql*net	Oracle SQL*NET
67	tcp, udp	bootpc	DHCP/BOOTP Protocol Server
68	tcp, udp	bootpc	DHCP/BOOTP Protocol Server
69	udp	tftp	Trivial File Transfer
70	tcp, udp	gopher	Gopher
71	tcp, udp	netrjs-1	Remote Job Service
72	tcp, udp	netrjs-2	Remote Job Service
73	tcp, udp	netrjs-3	Remote Job Service
74	tcp, udp	netrjs-4	Remote Job Service
75	udp		Any private dial out service
76	tcp, udp		Unassigned
77	tcp, udp		Any private RJE service
78	tcp, udp	vettcp	Vettcp
79	tcp, udp	finger	Finger
80	tcp, udp	www	World Wide Web HTTP
81	tcp, udp	hosts2-ns	HOSTS2 Name Server
82	tcp, udp	xfer	XFER Utility
83	tcp, udp	mit-ml-dev	MIT ML Device
84	tcp, udp	ctf	Common Trace Facility
85	tcp, udp	mit-ml-dev	MIT ML Device
86	tcp, udp	mfcobol	Micro Focus Cobol
87	tcp, udp		Any private terminal link; alias=ttylink
88	tcp, udp	kerberos	Kerberos
89	tcp	su-mit-tg	SU/MIT Telnet Gateway
89	udp	su-mit-tg	SU/MIT Telnet Gateway
90	tcp, udp		DNSIX Security Attribute Token Map

91	tcp, udp	mit-dov	MIT Dover Spooler
92	tcp, udp	npp	Network Printing Protocol
93	tcp, udp	dcp	Device Control Protocol
94	tcp, udp	objcall	Tivoli Object Dispatcher
95	tcp, udp	supdup	SUPDUP
96	tcp, udp	dixie	DIXIE Protocol Specification
97	tcp, udp	swift-rvf	Swift Remote Virtual File Protocol
98	tcp, udp	tacnews	TAC News
99	tcp, udp	metagram	Metagram Relay
100	tcp	newacct	[unauthorized use]
101	tcp, udp	hostname	NIC Host Name Server; alias=hostname
102	tcp, udp	iso-tsap	ISO-TSAP
103	tcp, udp	gppitnp	Genesis Point-to-Point Trans Net; alias=webster
104	tcp, udp	acr-nema	ACR-NEMA Digital Imag. & Comm. 300
105	tcp, udp	csnet-ns	Mailbox Name Nameserver
106	tcp, udp	3com-tsmux	3COM-TSMUX
107	tcp, udp	rtelnet	Remote Telnet Service
108	tcp, udp	snagas	SNA Gateway Access Server
109	tcp, udp	pop2	Post Office Protocol - Version 2; alias=postoffice
110	tcp, udp	pop3	Post Office Protocol - Version 3; alias=postoffice
111	tcp, udp	sunrpc	SUN Remote Procedure Call
112	tcp, udp	mcidas	McIDAS Data Transmission Protocol
113	tcp, udp	auth	Authentication Service; alias=authentication
114	tcp, udp	audionews	Audio News Multicast
115	tcp, udp	sftp	Simple File Transfer Protocol
116	tcp, udp	ansanotify	ANSA REX Notify
117	tcp, udp	uucp-path	UUCP Path Service
118	tcp, udp	sqlserv	SQL Services
119	tcp, udp	nntp	Network News Transfer Protocol; alias=usenet
120	tcp, udp	cfdptkt	CFDPTKT
121	tcp, udp	erpc	Encore Expedited Remote Pro.Call
122	tcp, udp	smakynet	SMAKYNET
123	tcp, udp	ntp	Network Time Protocol; alias=ntpd ntp
124	tcp, udp	ansatrader	ANSA REX Trader
125	tcp, udp	locus-map	Locus PC-Interface Net Map Server
126	tcp, udp	unitary	Unisys Unitary Login
127	tcp, udp	locus-con	Locus PC-Interface Conn Server
128	tcp, udp	gss-xlicen	GSS X License Verification
129	tcp, udp	pwdgen	Password Generator Protocol
130	tcp, udp	cisco-fna	Cisco FNATIVE
131	tcp, udp	cisco-tna	Cisco TNATIVE
132	tcp, udp	cisco-sys	Cisco SYSMAINT
133	tcp, udp	statsrv	Statistics Service
134	tcp, udp	ingres-net	INGRES-NET Service
135	tcp, udp	loc-srv	Location Service
136	tcp, udp	profile	PROFILE Naming System
137	tcp, udp	netbios-ns	NetBIOS Name Service
138	tcp, udp	netbios-dgm	NetBIOS Datagram Service
139	tcp, udp	netbios-ssn	NetBIOS Session Service
140	tcp, udp	emfis-data	EMFIS Data Service
141	tcp, udp	emfis-cntl	EMFIS Control Service
142	tcp, udp	bl-idm	Britton-Lee IDM
143	tcp, udp	imap2	Interim Mail Access Protocol v2
144	tcp, udp	news	NewS; alias=news
145	tcp, udp	uaac	UAAC Protocol
146	tcp, udp	iso-ip0	ISO-IP0

147	tcp, udp	iso-ip	ISO-IP
148	tcp, udp	cronus	CRONUS-SUPPORT
149	tcp, udp	aed-512	AED 512 Emulation Service
150	tcp, udp	sql-net	SQL-NET
151	tcp, udp	hems	HEMS
152	tcp, udp	bftp	Background File Transfer Program
153	tcp, udp	sgmp	SGMP; alias=sgmp
154	tcp, udp	netsc-prod	Netscape
155	tcp, udp	netsc-dev	Netscape
156	tcp, udp	sqlsrv	SQL Service
157	tcp, udp	knet-cmp	KNET/VM Command/Message Protocol
158	tcp, udp	pcmail-srv	PCMail Server; alias=repository
159	tcp, udp	nss-routing	NSS-Routing
160	tcp, udp	sgmp-traps	SGMP-TRAPS
161	tcp, udp	snmp	SNMP; alias=snmp
162	tcp, udp	snmptrap	SNMPTRAP
163	tcp, udp	cmip-man	CMIP/TCP Manager
164	tcp, udp	cmip-agent	CMIP/TCP Agent
165	tcp, udp	xns-courier	Xerox
166	tcp, udp	s-net	Sirius Systems
167	tcp, udp	namp	NAMP
168	tcp, udp	rsvd	RSVD
169	tcp, udp	send	SEND
170	tcp, udp	print-srv	Network PostScript
171	tcp, udp	multiplex	Network Innovations Multiplex
172	tcp, udp	cl/1	Network Innovations CL/1
173	tcp, udp	xyplex-mux	Xyplex
174	tcp, udp	mailq	MAILQ
175	tcp, udp	vmnet	VMNET
176	tcp, udp	genrad-mux	GENRAD-MUX
177	tcp, udp	xdmcp	X Display Manager Control Protocol
178	tcp, udp	nextstep	NextStep Window Server
179	tcp, udp	bgp	Border Gateway Protocol
180	tcp, udp	ris	Intergraph
181	tcp, udp	unify	Unify
182	tcp, udp	audit	Unisys Audit SITP
183	tcp, udp	ocbinder	OCBinder
184	tcp, udp	ocserver	OCServer
185	tcp, udp	remote-kis	Remote-KIS
186	tcp, udp	kis	KIS Protocol
187	tcp, udp	aci	Application Communication Interface
188	tcp, udp	mumps	Plus Five's MUMPS
189	tcp, udp	qft	Queued File Transport
190	tcp, udp	gacp	Gateway Access Control Protocol
191	tcp, udp	prospero	Prospero
192	tcp, udp	osu-nms	OSU Network Monitoring System
193	tcp, udp	srmp	Spider Remote Monitoring Protocol
194	tcp, udp	irc	Internet Relay Chat Protocol
195	tcp, udp	dn6-nlm-aud	DNSIX Network Level Module Audit
196	tcp, udp	dn6-smm-red	DNSIX Session Mgt Module Audit Redir
197	tcp, udp	dls	Directory Location Service
198	tcp, udp	dls-mon	Directory Location Service Monitor
199	tcp, udp	smux	SMUX
200	tcp, udp	src	IBM System Resource Controller
201	tcp, udp	at-rtmp	AppleTalk Routing Maintenance
202	tcp, udp	at-nbp	AppleTalk Name Binding

203	tcp, udp	at-3	AppleTalk Unused
204	tcp, udp	at-echo	AppleTalk Echo
205	tcp, udp	at-5	AppleTalk Unused
206	tcp, udp	at-zis	AppleTalk Zone Information
207	tcp, udp	at-7	AppleTalk Unused
208	tcp, udp	at-8	AppleTalk Unused
209	tcp, udp	tam	Trivial Authenticated Mail Protocol
210	tcp, udp	z39.50	ANSI Z39.50
211	tcp, udp	914c/g	Texas Instruments 914C/G Terminal
212	tcp, udp	anet	ATEXSSTR
213	tcp, udp	ipx	IPX
214	tcp, udp	vmpwscs	VM PWSCS
215	tcp, udp	softpc	Insignia Solutions
216	tcp, udp	atls	Access Technology License Server
217	tcp, udp	dbase	dBASE UNIX
218	tcp, udp	mpp	Netix Message Posting Protocol
219	tcp, udp	uarps	Unisys ARPs
220	tcp, udp	imap3	Interactive Mail Access Protocol v3
221	tcp, udp	fln-spx	Berkeley rlogind with SPX auth
222	tcp, udp	fsh-spx	Berkeley rshd with SPX auth
223	tcp, udp	cdc	Certificate Distribution Center
224-241			Reserved
243	tcp, udp	sur-meas	Survey Measurement
245	tcp, udp	link	LINK
246	tcp, udp	dsp3270	Display Systems Protocol
247-255			Reserved
345	tcp, udp	pawserv	Perf Analysis Workbench
346	tcp, udp	zserv	Zebra server
347	tcp, udp	fatserv	Fatmen Server
371	tcp, udp	clearcase	Clearcase
372	tcp, udp	ulistserv	UNIX Listserv
373	tcp, udp	legent-1	Legent Corporation
374	tcp, udp	legent-2	Legent Corporation
512	tcp	print	Windows NT Server and Windows NT Workstation version 4.0 can send LPD client print jobs from any available reserved port between 512 and 1023. See also description for ports 721 to 731.
512	udp	biff	Used by mail system to notify users of new mail received; currently receives messages only from processes on the same computer; alias=comsat
513	tcp	login	Remote logon like telnet; automatic authentication performed, based on privileged port numbers and distributed databases that identify authentication domains
513	udp	who	Maintains databases showing who's logged on to the computers on a local net and the load average of the computer; alias=whod
514	tcp	cmd	Like exec, but automatic authentication is performed as for logon server
514	udp	syslog	
515	tcp, udp	printer	Spooler; alias=spooler. The print server LPD service will listen on tcp port 515 for incoming connections.
517	tcp, udp	talk	Like tenex link, but across computers; unfortunately, doesn't use link protocol (this is actually just a rendezvous port from which a TCP connection is established)
518	tcp, udp	ntalk	
519	tcp, udp	utime	Unixtime

520	tcp	efs	Extended file name server
520	udp	router	Local routing process (on site); uses variant of Xerox NS routing information protocol;alias=router routed
525	tcp, udp	timed	Timeserver
526	tcp, udp	tempo	Newdate
530	tcp, udp	courier	RPC
531	tcp	conference	Chat
531	udp	rvd-control	MIT disk
532	tcp, udp	netnews	Readnews
533	tcp, udp	netwall	For emergency broadcasts
540	tcp, udp	uucp	Uucpd
543	tcp, udp	klogin	
544	tcp, udp	kshell	Krcmd; alias=cmd
550	tcp, udp	new-rwho	New-who
555	tcp, udp	dsf	
556	tcp, udp	remotefs	Rfs server; alias=rfs_server rfs
560	tcp, udp	rmonitor	Rmonitord
561	tcp, udp	monitor	
562	tcp, udp	chshell	Chcmd
564	tcp, udp	9pfs	Plan 9 file service
565	tcp, udp	whoami	Whoami
570	tcp, udp	meter	Demon
571	tcp, udp	meter	Udemon
600	tcp, udp	ipcserver	Sun IPC server
607	tcp, udp	nqs	Nqs
666	tcp, udp	mdqs	
704	tcp, udp	elcsd	Errlog copy/server daemon
721-731	tcp	printer	Under Windows NT 3.5x, all TCP/IP print jobs sent from a Windows NT computer were sourced from TCP ports 721 through 731. This is changed for Windows NT Server and Windows NT Workstation version 4.0, which sources LPD client print jobs from any available reserved port between 512 and 1023.
740	tcp, udp	netcp	NETscout Control Protocol
741	tcp, udp	netgw	NetGW
742	tcp, udp	netrcs	Network based Rev. Cont. Sys.
744	tcp, udp	flexlm	Flexible License Manager
747	tcp, udp	fujitsu-dev	Fujitsu Device Control
748	tcp, udp	ris-cm	Russell Info Sci Calendar Manager
749	tcp, udp	kerberos-adm	Kerberos administration
750	tcp	rfile	Kerberos authentication; alias=kdc
750	udp	loadav	
751	tcp, udp	pump	Kerberos authentication
752	tcp, udp	qrh	Kerberos password server
753	tcp, udp	rrh	Kerberos userreg server
754	tcp, udp	tell	Send; Kerberos slave propagation
758	tcp, udp	nlogin	
759	tcp, udp	con	
760	tcp, udp	ns	
761	tcp, udp	rxe	
762	tcp, udp	quotad	
763	tcp, udp	cycleserv	
764	tcp, udp	omserv	
765	tcp, udp	webster	
767	tcp, udp	phonebook	Phone
769	tcp, udp	vid	
770	tcp, udp	cadlock	

771	tcp, udp	rtip	
772	tcp, udp	cycleserv2	
773	tcp	submit	
773	udp	notify	
774	tcp	rpasswd	
774	udp	acmaint_dbd	
775	tcp	entomb	
775	udp	acmaint_transd	
776	tcp, udp	wpages	
780	tcp, udp	wpgs	
781	tcp, udp	hp-collector	HP performance data collector
782	tcp, udp	hp-managed-node	HP performance data managed node
783	tcp, udp	hp-alarm-mgr	HP performance data alarm manager
800	tcp, udp	mdbs_daemon	
801	tcp, udp	device	
888	tcp	erlogin	Logon and environment passing
996	tcp, udp	xtreelic	XTREE License Server
997	tcp, udp	maitrd	
998	tcp	busboy	
998	udp	puparp	
999	tcp	garcon	
999	udp	applix	Applix ac
999	tcp, udp	puprouter	
1000	tcp	cadlock	
1000	udp	ock	

Registered Port Assignments

The registered ports are not controlled by the IANA and on most systems can be used by user processes or programs. Registered ports between 1024 and 5000 are also referred to as the ephemeral ports. Although the IANA cannot control uses of these ports, it does register or list uses of these ports as a convenience to the TCP/IP community. To the extent possible, these same port assignments are used with UDP. The registered ports are in the range 1024 - 65535.

This list specifies the port used by the Windows NT Server and Windows NT Workstation server process as its contact port for services and third-party software.

Information

Programs that use Remote Procedure Call (RPC) to communicate can randomly select a registered port above 1024.

Port	*Protocol*	*Service Name*	*Alias*
1024			Reserved
1025	tcp, udp	blackjack	Network blackjack
1109	tcp	kpop	Pop with Kerberos
1167	udp	phone	
1248	tcp, udp	hermes	
1347	tcp, udp	bbn-mmc	Multimedia conferencing
1348	tcp, udp	bbn-mmx	Multimedia conferencing
1349	tcp, udp	sbook	Registration Network Protocol
1350	tcp, udp	editbench	Registration Network Protocol
1351	tcp, udp	equationbuilder	Digital Tool Works (MIT)
1352	tcp, udp	lotusnote	Lotus Note
1512	tcp, udp	WINS	Reserved for future use for Microsoft Windows Internet Name Service
1524	tcp, udp	ingreslock	Ingres
1525	tcp, udp	orasrv	Oracle
1525	tcp, udp	prospero-np	Prospero nonprivileged
1527	tcp, udp	tlisrv	Oracle
1529	tcp, udp	coauthor	Oracle
1600	tcp, udp	issd	
1650	tcp, udp	nkd	
1666	udp	maze	
2000	tcp, udp	callbook	
2001	tcp	dc	
2001	udp	wizard	Curry
2002	tcp, udp	globe	
2004	tcp	mailbox	
2004	udp	emce	CCWS mm conf
2005	tcp	berknet	
2005	udp	oracle	
2006	tcp	invokator	
2006	udp	raid-cc	RAID
2007	tcp	dectalk	
2007	udp	raid-am	
2008	tcp	conf	
2008	udp	terminaldb	
2009	tcp	news	
2009	udp	whosockami	
2010	tcp	search	
2010	udp	pipe_server	
2011	tcp	raid-cc	RAID
2011	udp	servserv	

2012	tcp	ttyinfo	
2012	udp	raid-ac	
2013	tcp	raid-am	
2013	udp	raid-cd	
2014	tcp	troff	
2014	udp	raid-sf	
2015	tcp	cypress	
2015	udp	raid-cs	
2016	tcp, udp	bootserver	
2017	tcp	cypress-stat	
2017	udp	bootclient	
2018	tcp	terminaldb	
2018	udp	rellpack	
2019	tcp	whosockami	
2019	udp	about	
2020	tcp, udp	xinupageserver	
2021	tcp	servexec	
2021	udp	xinuexpansion1	
2022	tcp	down	
2022	udp	xinuexpansion2	
2023	tcp, udp	xinuexpansion3	
2024	tcp, udp	xinuexpansion4	
2025	tcp	ellpack	
2025	udp	xribs	
2026	tcp, udp	scrabble	
2027	tcp, udp	shadowserver	
2028	tcp, udp	submitserver	
2030	tcp, udp	device2	
2032	tcp, udp	blackboard	
2033	tcp, udp	glogger	
2034	tcp, udp	scoremgr	
2035	tcp, udp	imsldoc	
2038	tcp, udp	objectmanager	
2040	tcp, udp	lam	
2041	tcp, udp	interbase	
2042	tcp, udp	isis	
2043	tcp, udp	isis-bcast	
2044	tcp, udp	rimsl	
2045	tcp, udp	cdfunc	
2046	tcp, udp	sdfunc	
2047	tcp, udp	dls	
2048	tcp, udp	dls-monitor	
2049	tcp, udp	shilp	Sun NFS
2053	tcp	knetd	Kerberos de-multiplexer
2105	tcp	eklogin	Kerberos encrypted rlogon
2784	tcp, udp	www-dev	World Wide Web - development
3049	tcp, udp	NSWS	
4672	tcp, udp	rfa	Remote file access server
5000	tcp, udp	commplex-main	
5001	tcp, udp	commplex-link	
5002	tcp, udp	rfe	Radio Free Ethernet
5145	tcp, udp	rmonitor_secure	
5236	tcp, udp	padl2sim	
5555	tcp	rmt	Rmtd
5556	tcp	mtb	Mtbd (mtb backup)
6111	tcp, udp	sub-process	HP SoftBench Sub-Process Control

6558	tcp, udp	xdsxdm	
7000	tcp, udp	afs3-fileserver	File server itself
7001	tcp, udp	afs3-callback	Callbacks to cache managers
7002	tcp, udp	afs3-prserver	Users and groups database
7003	tcp, udp	afs3-vlserver	Volume location database
7004	tcp, udp	afs3-kaserver	AFS/Kerberos authentication service
7005	tcp, udp	afs3-volser	Volume management server
7006	tcp, udp	afs3-errors	Error interpretation service
7007	tcp, udp	afs3-bos	Basic overseer process
7008	tcp, udp	afs3-update	Server-to-server updater
7009	tcp, udp	afs3-rmtsys	Remote cache manager service
9535	tcp, udp	man	Remote man server
9536	tcp	w	
9537	tcp	mantst	Remote man server, testing
10000	tcp	bnews	
10000	udp	rscs0	
10001	tcp	queue	
10001	udp	rscs1	
10002	tcp	poker	
10002	udp	rscs2	
10003	tcp	gateway	
10003	udp	rscs3	
10004	tcp	remp	
10004	udp	rscs4	
10005	udp	rscs5	
10006	udp	rscs6	
10007	udp	rscs7	
10008	udp	rscs8	
10009	udp	rscs9	
10010	udp	rscsa	
10011	udp	rscsb	
10012	tcp	qmaster	
10012	udp	qmaster	
17007	tcp, udp	isode-dua	

THE RESOURCE KIT UTILITIES

The following are Microsoft sanctioned utilities that install with the Windows NT 4.0 Resource Kits. This should be used as a quick overview of the utilities available, and a brief description of their functionality. Always read fully the respective documentation for a full explanation of features before attempting to use them.

Program	*Usage*	*Location*
3DPAINT.EXE	3DPAINT is a paint utility that enables you to create three-dimensional bitmap graphics.	GUI
ADDUSERS.EXE	Add Users for Windows NT is a 32-bit administrative command-line tool used to create or write user accounts to a comma-delimited file. Add Users is most beneficial when the file is maintained in a spreadsheet, such as Microsoft Excel, that will work with comma-delimited files. Typical use includes the batch creation of multiple NT user accounts.	COMMAND-LINE
ANIEDIT.EXE	Microsoft Animated Cursor Editor. Use the animated cursor creator to draw and edit frames to create animated cursors.	GUI
APIMON.EXE	This command-line tool enables the user to monitor the API calls a process is making. APIMON incorporates the functionality of Application Profiler, which is being dropped from the Windows NT 4.0 Resource Kit.	COMMAND-LINE
ASSOCIATE.EXE	This command-line utility enables you to register or un-register a filename extension with the Registry. "File extension, executable program" associations enable the Windows NT 4.0 shell to start the correct executable program when a file with the associated extension is opened from the command line or from Explorer.	COMMAND-LINE
ATANLYZR.EXE	ATANLYZR performs an AppleTalk lookup for registered AppleTalk devices on an AppleTalk network. The user can perform a lookup of all AppleTalk devices, specific Net, Name, Type, or partial Name, and Types in the selected zone(s).	
AUDITCAT.HLP	This Windows Help file displays information on seven categories of audit events.	HELP FILE
AUTOEXNT.EXE	The AutoExNT service allows you to start a batch file, AUTOEXNT.BAT, at boot time without having to log on to the computer on which it will run.	COMMAND-LINE
AUTOLOG.EXE	Windows NT Auto Logon Setter is a simple GUI utility which configures a Windows NT Workstation to automatically log on a particular user at bootup. This enables you to bypass the CTRL+ALT+DEL logon dialog box.	GUI
BREAKFTM.EXE	This command-line utility was designed to be used with Windows NT Server 4.0 Unattended Upgrade. Windows NT computers that have the system drive mirrored cannot be upgraded, as a mirrored system drive will cause the Unattended Upgrade to fail. The mirror must therefore be broken before upgrading. BREAKFTM breaks the system mirror before the Windows NT Server 4.0 upgrade, and then recreates the mirror once the upgrade is finished. The tool has no effect on computers that do not have a system mirror.	COMMAND-LINE NT SERVER ONLY

BROWMON.EXE	The Browser Monitor is a Windows-based utility that monitors the status of browsers on selected domains. Browsers are shown on a per-domain and per-transport basis.	GUI
BROWSTAT.EXE	BrowStat is a general purpose, character-based browser diagnostic. Use BrowStat to find whether a browser is running and to find active Microsoft Windows for Workgroups 1.0 (WFW) browsers in Windows NT domains. This utility provides information about the state of the browser in a workgroup, including the name of the master browser.	COMMAND-LINE
C2CONFIG.EXE	The Windows NT C2 Configuration Manager displays the various C2 security parameters and their current configuration. Selecting one of these items will display more information on the configuration of that item and allow you to change the configuration as desired.	GUI
CAT.EXE	Posix utility that reads files sequentially, writing them to the standard output.	COMMAND-LINE
CHMOD.EXE	Posix utility that modifies the file mode bits of the listed files as specified by the mode operand.	COMMAND-LINE
CHOICE.EXE	CHOICE prompts the user to make a choice in a batch program by displaying a prompt and pausing for the user to choose from among a set of keys. You can use this command only in batch programs.	COMMAND-LINE
CHOWN.EXE	Posix utility to change the owner of a file.	COMMAND-LINE
CLIP.EXE	CLIP.EXE dumps STDIN to the Windows NT Clipboard. Run any program that prints text to STDOUT and pipe the results through Clip. Clip will read from its STDIN and copy the text to the Clipboard.	COMMAND-LINE
COMPREG.EXE	A Win32 character-based/command-line "Registry DIFF" that enables you to compare any two local and/or remote Registry keys in both Windows NT and Windows 95.	COMMAND-LINE
COMPRESS.EXE	This command-line utility can be used to compress one or more files.	COMMAND-LINE
CP.EXE	Posix command to copy files.	COMMAND-LINE
Crystal Reports for NT Resource Kit	Windows-based WYSIWYG report writer for formatting reports from the NT Event Log. Included are a number of sample reports that can be refreshed with data from the local machine.	MULTI-FILE APPLICATION
DATALOG.EXE	The Performance Monitor Service, invoked by the MONITOR.EXE utility. This service runs on the computer on which it is started. Alerts are watched locally on that computer, so no data needs to travel across the network.	COMMAND-LINE
dbWeb	dbWeb is a gateway between Microsoft Open Database Connectivity (ODBC) data sources and the Internet Information Server (IIS). You can use dbWeb to publish data from an ODBC data source and provide familiar World Wide Web (WWW) hypertext navigation. While allowing users to create queries, dbWeb enables you to filter the data and sources users can access and display.	GUI
DELPROF.EXE	This command-line utility deletes user profiles on Windows NT computers.	COMMAND-LINE
DELSRV.EXE	This command-line utility un-registers a service with the service control manager.	COMMAND-LINE
Designed for Windows NT and Windows 95 Logo Handbook (WINLOGO.DOC)	The "Designed for Windows NT and Windows 95 Logo Handbook for Software Applications" describes the technical requirements that must be satisfied by an application in order to receive the Designed for Windows NT and Windows 95 logo	

Desktop Themes	Desktop Themes include a variety of visual, sound, and symbolic components that can enhance the look and feel of your Windows NT 4.0 desktop. Each desktop theme includes a background wallpaper, a screen saver, a color scheme, and a set of sounds, cursors, icons, and fonts.	UI ENHANCEMENTS
DESKTOPS.EXE	This desktop-switching application for Windows NT 4.0 enables you to customize desktop wallpaper and colors and separate executing programs into new deskspaces.	GUI
DFLAYOUT.EXE	This layout tool for document files enables you to optimize compound files for better performance on the World Wide Web.	GUI
DH.EXE	This command-line utility enables your to lock heaps, tags, stacks, and objects.	COMMAND-LINE
DHCPCMD.EXE	The command-line DHCP Administrator's Tool is an auxiliary method of administering DHCP servers.	COMMAND-LINE
DHCPLOC.EXE	DHCPLOC.EXE displays the DHCP servers active on the subnet. It beeps and sends out alert messages if it detects any unauthorized DHCP servers. It also displays packets it detects from DHCP servers; you can specify whether it displays packets from all DHCP servers, or only from unauthorized servers.	COMMAND-LINE
DIRUSE.EXE	This utility will traverse the named directory and it's subs to give you disk space usage for the specified directory tree.	COMMAND-LINE
DISKMAP.EXE	This command-line utility produces a detailed report on the configuration of the hard disk that you specify. It provides information from the Registry about disk characteristics and geometry, and reads and displays data about all of the partitions and logical drives defined on the disk.	COMMAND-LINE
DSKPROBE.EXE	DiskProbe is a sector editor for Windows NT Server and Workstation. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way. You can use DiskProbe to replace the Master Boot Record, repair damaged partition table information and to repair or replace damaged Partition Boot Sectors or other file system data. The program can also save Master Boot Records and Partition Boot Sectors as files. They can then be replaced if the sectors become damaged at a later time. These on-disk data structures are not accessible through the file system, and so are not saved by any backup programs currently available.	GUI
DISKSAVE.EXE	DISKSAVE allows you to save the Master Boot Record and Partition Boot Sector as binary image files. Once these critical disk structures have been saved, they can be easily restored if they become corrupted later on. This tool also enables you to disable fault tolerance on the Boot Drive, which can be useful when Windows NT will not boot from a mirrored system drive.	COMMAND-LINE
DNSSTAT.EXE	This command-line utility provides a dump of DNS server statistics (queries and responses, database size, caching, memory consumption) on a computer running Microsoft DNS Server.	COMMAND-LINE
DOMMON.EXE	Domain Monitor is a Windows-based utility that monitors the status of servers in a domain and the secure channel status to the domain controller and to domain controllers in trusted domains. Domain Monitor displays various status errors, plus the domain controller name and a list of trusted domains.	GUI

DRIVERS.EXE	The Drivers tool displays character-based information about the installed device drivers. There are no command-line arguments.	COMMAND-LINE
DSKPROBE.EXE	DiskProbe is a sector editor for Windows NT Server and Workstation. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way.	GUI
DUMPEL.EXE	Dump Event Log is a command-line utility that can be used to dump an event log for a local or remote system into a tab-separated text file. This utility can also be used to filter for certain event types or to filter out certain event types.	COMMAND-LINE
EM2MS.EXE	This command-line utility converts verbose descriptions of files stored on NT-based EMWAC (European Microsoft Windows NT Academic Centre) Gopher Servers to the Microsoft Internet Information Gopher Server content format. EM2MS.EXE is useful for EMWAC Gopher Server administrators who want to begin using the Microsoft Internet Information Gopher Server. It allows them to easily convert their EMWAC-based content descriptions to the Microsoft Gopher tag-file format.	COMMAND-LINE
EMWAC Server CGI Gateway Scripts	A gateway script is an executable program that uses the CGI protocol, Common Gateway Interface, to communicate with a server on the World-Wide Web. Gateway scripts add custom features to a Web server, increasing the diversity of services that a Web server can provide to the Web browser. The example gateway script provided in the Resource Kit demonstrates how to provide access to the Microsoft SQL Server. The script accepts a single SQL statement, which it passes on to SQL Server. The results, including any error messages, are returned to the browser for display to the user.	COMMAND-LINE
ENUMPRN.EXE	Windows utility to display installed printer drivers.	GUI
EXCTRLST.EXE	This utility provides information on the Extensible Performance Counter DLLs that have been installed on a Windows NT computer, listing the services and applications that provide performance information via the Windows NT Registry. You can use these performance counters for optimizing and troubleshooting.	COMMAND-LINE
EXETYPE.EXE	ExeType is an MS-DOS-based application that identifies the operating system environment and processor required to run a particular executable file.	COMMAND-LINE
EXPNDW32.EXE	You can use the File Expansion Utility to expand one or more compressed files from the Windows NT CD. EXPNDW32.EXE is a 32-bit utility that provides a fully graphical interface for ease of use.	COMMAND-LINE
FIND.EXE	Find recursively descends the directory tree for each file listed, evaluating an expression (composed of a rich set of arguments) in terms of each file in the tree.	COMMAND-LINE
FINDGRP.EXE	The Find Group utility finds all direct and indirect group memberships for a specified user in a domain. This helps determine a particular users access to Windows NT Domain Controllers in a domain by listing the groups in which the user is a member.	COMMAND-LINE
FLOPLOCK.EXE	FloppyLock is a service that controls access to the floppy drives of a computer. When the service is started on Windows NT Workstation, only members of the Administrators and Power Users groups can access the floppy drives. When the service is started on Windows NT Server, only members of the Administrators group can access the floppy drives. Install via INSTSRV.EXE.	SERVICE

FORFILES.EXE	This command-line utility can be used in a batch file to select files in a folder or tree for batch processing. FORFILES enable you to run a command on or pass arguments to multiple files. For example, you could run the TYPE command on all files in a tree with the *.TXT extension. Or you could execute every batch file (*.BAT) on the C:\ drive with the filename "MYINPUT.TXT" as the first argument.	COMMAND-LINE
FREEDISK.EXE	This command-line utility checks for free disk space, returning a 0 If there is enough space and a 1 if there isn't.	COMMAND-LINE BATCH/SCRIPT
FTEDIT.EXE	FTEDIT.EXE is a new GUI utility that allows you to create, edit, and delete fault tolerance sets for disk drives and partitions of local and remote computers. It improves on the functionality of the command-line utility SHOWDISK.EXE.	GUI
FTPCONF.EXE	Windows-based utility to configure your Microsoft FTP Server.	GUI
GETMAC.EXE	Command-line utility to display network transports and address information.	COMMAND-LINE
GETSID.EXE	This utility which returns the SID information for any two system accounts.	COMMAND-LINE
GLOBAL.EXE	This command-line utility displays members of global groups on remote servers or domains.	COMMAND-LINE
GREP.EXE	Posix utility (Global Regular Expression Print) to search one or more files for lines that match a regular expression.	COMMAND-LINE
GRPCOPY.EXE	This GUI utility enables users to copy the usernames in an existing group to another group in the same or another domain or on a Windows NT computer. It is included in the Windows NT Server Resource Kit only.	GUI
GRPTOREG.EXE	This tool creates group files for Program Manager and converts them to the Registry for use in Windows NT.	COMMAND-LINE
HCL40.HLP	Hardware Compatibility List in Windows Help format.	HELP FILE
HEAPMON.EXE	This command-line tool enables the user to view system heap information.	COMMAND-LINE
IFMEMBER.EXE	IfMember is a command-line utility that checks whether the current user is a member of a specified group. It is typically used in Windows NT Workstation and Windows NT Server logon scripts and other batch files.	COMMAND-LINE
IMAGEDIT.EXE	The Image Editor allows you to create and edit cursors and icons for VGA, monochrome, and other display devices. The Image Editor is also used with aniedit.exe to create custom animated cursors.	GUI

Index Server	Index Server is the Microsoft content-indexing and searching solution for Microsoft Internet Information Server (IIS), which is included with Windows NT Server 4.0, and Peer Web Services (PWS), which is included with Windows NT Workstation 4.0. An add-on module for IIS and PWS, Index Server is designed to index the full text and properties of documents on an IIS or PWS-based server. Index Server can index documents for both corporate intranets and for any drive accessible through an uniform naming convention (UNC) path on the Internet. Clients can formulate queries by using any World Wide Web (WWW) browser to fill in the fields of a simple Web query form. The Web server forwards the query form to the query engine, which finds the pertinent documents and returns the results to the client formatted as a Web page. Unlike many content indexing systems, Index Server can index the text and properties of formatted documents, such as those created by Microsoft® Word or Microsoft® Excel. This feature lets you publish existing documents on your intranet Web without converting them to HyperText Markup Language (HTML).	MULTI-FILE APPLICATION NT SERVER ONLY
INET.EXE	INET is a network command that works like the Windows NT NET command, except that UNC names are assumed to be Internet Domain Name Server (DNS) names and translated accordingly. Inet works on TCP/IP services rather than on SMB.	COMMAND-LINE
INSTALL.CMD	INSTALLD.CMD installs NTDETECT.CHK, the debug or checked version of NTDETECT.COM, from the Windows NT CD.	See related topic NTDETECT.COM
INSTSRV.EXE	INSTSRV.EXE: Service Installer is a command-line utility that installs and uninstalls executable (.EXE) services and assigns names to them.	COMMAND-LINE
KERNPROF.EXE	This command-line utility provides counters for and profiles of various functions of the Windows NT operating system Kernel. With Kernel Profiler, you can monitor details and frequency for each function the Kernel calls, how often a process switches from User mode to Kernel mode, and, on a multi-processor computer, display information for each processor.	COMMAND-LINE
KILL.EXE	KILL.EXE is a command-line utility you can use to end one or more tasks, or processes. When using KILL.EXE, you can specify a process by its process ID number, any part of its process name, or its window title, if it has a window. You can use the TLIST.EXE utility, also included with this Resource Kit, to find the process names and process IDs of currently running processes.	COMMAND-LINE
KIX32.EXE	KiXtart 95 is a logon script processor and/or enhanced batch language for Windows NT and Windows 95 workstations in a Windows Networking environment.	BATCH/SCRIPT
LAYOUT.DLL	This utility is a shell extension that saves and restores the icon positions on a desktop.	EXPLORER EXTENSION
LN.EXE	Posix utility which allows you to create pseudonyms (links) for files, allowing them to be accessed by different names.	COMMAND-LINE
LOCAL.EXE	This command-line utility displays members of local groups on remote servers or domains.	COMMAND-LINE
LOGEVENT.EXE	LogEvent enables entries to be made to the Windows NT Event Log on either the local or a remote machine from the command line or a batch file.	COMMAND-LINE

LOGTIME.EXE	A command-line tool that logs the start or finish of command-line programs from a batch file. This can be useful for timing and tracking batch jobs such as mail-address imports.	COMMAND-LINE
LS.EXE	Posix utility to list files.	COMMAND-LINE
Mail Server	Mail Server is an SMTP and POP server for Windows NT. The intermediate files and the mailboxes are all spooled securely (when using the NTFS file system) on the computer running Windows NT server, and can be accessed by any POP-compliant public-domain (PD) or commercial client.	MULTI-FILE APPLICATION
MIBCC.EXE	MIB (Management Information Base) compiler for SNMP (Simple Network Management Protocol).	COMMAND-LINE
MKDIR.EXE	Posix utility to create one or more directories.	COMMAND-LINE
MONITOR.EXE	Command-line interface to the Performance Monitor service. The activity being monitored is described in a workspace settings file that you create using Performance Monitor. You use monitor.exe to start, stop, and to establish a particular workspace settings file describing the measurement. You can run monitor.exe from a remote computer, so complete control of all your Performance Monitor services is available from any Windows NT computer on the network.	COMMAND-LINE
MUNGE.EXE	This utility provides a convenient way to search for and replace strings in a file.	COMMAND-LINE
MV.EXE	Posix utility to move file and directories or to rename them.	COMMAND-LINE
NETCLIP.EXE	NetClip is a GUI utility that enables you to view the contents of another computer's clipboard, and to Drag & Drop (or Cut & Paste) any data, in any format, to and from the other computer.	GUI
NETSVC.EXE	Command-line utility which remotely controls and displays status of a specified service on a given computer.	COMMAND-LINE
NetTime for Macintosh	This Macintosh program synchronizes the local Macintosh clock to a given AppleShare server on the network. It requires ResEdit or another resource editor to change the zone and server name for the tool to synchronize to.	MACINTOSH
NETWATCH.EXE	Windows-based utility which provides general system, user, share and file information on local and remote resources.	GUI
NLMON.EXE	This command-line utility can be used to list and test many aspects of Trust relationships.	COMMAND-LINE
NLTEST.EXE	This command-line tool helps perform administrative tasks such as forcing a user-account database into sync, gettting a list of PDC's, forcing a shutdown, querying and checking on the status of trust.	COMMAND-LINE
NOW.EXE	Similar to ECHO, this command will display date and time stamp information followed by the given string argument. Useful in batch file debugging or possibly batch performance monitoring.	COMMAND-LINE
NTCARD40.HLP	Windows NT Adapter Card Help was created by Microsoft Product Support to assist you in the setup of network adapters, SCSI adapters, and sound cards for Windows NT 4.0. This file provides IRQ, I/O base, RAM base address, and other settings, along with illustrations that show the location for jumper settings on the cards.	HELP FILE
NTDETECT.COM	INSTALLD.CMD installs NTDETECT.CHK, the debug or checked version of NTDETECT.COM, from the Windows NT CD.	

NTUUCODE.EXE	NTUUCODE is a 32-bit GUI program that you can use to encode or decode files according to the UUEncoding standard.	GUI
OLEVIEW.EXE	This administration and testing tool for Microsoft Component Object Model (COM) classes is oriented towards developers and power users. The user interface, however, offers both "Expert" and "Novice" modes. OLE/COM Object Viewer enables you to browse, configure, activate, and test all of the COM classes installed on your computer. You can also configure system-wide COM settings, including enabling or disabling Distributed COM, and activate COM classes remotely. The new Component Categories specification is fully supported.	GUI
OS2API.TXT	The OS2API.TXT file contains information for developers describing which APIs for the OS/2 operating system are supported by Windows NT 4.0 and which are not supported.	DEVELOPER DOC
PASSPROP.EXE	This command-line tool can be used to set two domain policy flags: whether passwords have to be complex and whether the administrator account can be locked out. These domain password and security properties cannot be set by any other tool, including the NET command and User Manager.	COMMAND-LINE
PATHMAN.EXE	This command-line tool enables you to add or remove components of both the system and user paths. It can modify any number of paths in a single call and includes error checking that can handle path abnormalities such as repeated entries, adjacent semicolons, and missing entries.	COMMAND-LINE
PERF2MIB.EXE	Using PERF2MIB.EXE: Performance Monitor MIB Builder Tool, developers can create new ASN.1 syntax MIBs for their applications, services, or devices that use Performance Monitor counters. Administrators can then track performance of these components using any system-management program that supports SNMP.	COMMAND-LINE
PerfLog Data Log Service	This tool logs data from performance counters to tab or comma-separated variable files. It lets you choose which performance counters you want to log, and starts new log files automatically at intervals you select. The text files to which PerfLog logs data can be used as input to spreadsheets, databases, and other applications, as well as to Performance Monitor. Unlike Performance Monitor logs, which store data in a compact, multi-dimensional C-language data format, PerfLog logs can be used as direct input without reformatting. PerfLog uses the same objects and counters as Performance Monitor (included with the Windows NT operating system), but it lets you select which counters you want to log for each instance of an object. You can also select the level of detail you need on an instance and let PerfLog select a set of counters for you.	SERVICE
PERFMTR.EXE	Command-line performance monitor which displays CPU, memory, cache, and I/O usages, VdM and server statistics until user terminates the display.	COMMAND-LINE

Performance Tools	The \PERFTOOL folder of the installed Resource Kit contains tools for monitoring and optimizing the performance of a computer running Windows NT or a Windows NT application. Several of these tools are also covered in separate topics in this Help file. The Performance Tools are grouped into folders by function. A few of these tools are listed in more than one sub-folder. The \EXAMPLES folder is not installed by default because it contains over 20 MB of files.	
PERL	Practical Extraction and Report Language. Perl is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. It's also a good language for many system management tasks.	
PERMCOPY.EXE	This command-line utility copies file- and share-level permissions.	COMMAND-LINE
PERMS.EXE	Command-line utility which displays specified users' permissions for a given file.	COMMAND-LINE
PFMON.EXE	This utility enables you to monitor the page faults that occur as you run an application. Page Fault Monitor produces a running list of hard and soft page faults generated by each function call by the application.	COMMAND-LINE
PMON.EXE	Command-line utility which displays process statistics. Useful in troubleshooting system resource problems, etc..	COMMAND-LINE
POLEDIT.EXE	This utility sets administrative policies to override user behavior.	GUI
PSTAT.EXE	Version 0.2 of this command-line utility displays process statistics. Useful for debugging problems.	COMMAND-LINE
PULIST.EXE	This command-line tool tracks what processes are running on local or remote computers. It can list the names and process IDs of all processes running on one or more remote systems. If run against the local computer (with no arguments specified), PULIST will also try to list the user name associated with each process.	COMMAND-LINE
PVIEWER.EXE	Windows-based process management tool which allows for process termination and priority boosting and downgrading.	GUI
QSLICE.EXE	Windows-based tool which shows the amount of CPU used by each process in the system.	GUI
QUICKRES.EXE	This tool enables you to change the visible screen area, resolution (DPI), bit depth, and color palette settings from the taskbar, without restarting Windows NT.	GUI
QUICKRUN.EXE	This utility provides a convenient method of launching Windows applications.	GUI
RASLIST.EXE	This command-line utility displays RAS server announces from a network.	COMMAND-LINE
RASUSERS.EXE	RasUsers lets you list all user accounts that have been granted permission to dial in to the network via Remote Access Service (RAS).	COMMAND-LINE
RCMD.EXE	Remote Command allows a user to execute a single command on a remote server from within a command shell. If the command is supplied then the shell executes the command once before exiting the shell. If command is not supplied, it leaves the user in an interactive session until explicitly exited or session is otherwise broken.	COMMAND-LINE
REGBACK.EXE	Allows user with SeBackupPriviledge the ability to back up a servers' registry hives (without the use of tape) while they are in use. Options are available to back up a single hive or all at once. Error exit codes reflect success, failure or other. Recommended use prior to any changes to the registry.	COMMAND-LINE

REGCHG.EXE	This command-line utility makes changes to the Registry on the local or a remote system.	COMMAND-LINE
REGDEL.EXE	This command-line and batch utility removes Registry keys remotely or on the local computer.	COMMAND-LINE
REGENTRY.HLP	his tool provides a database of Windows NT Registry entries in the form of a Help file. You can use this Help file while working in Registry Editor to find ranges, minimum-maximum values, and instructions for setting specific values in the Registry.	HELP FILE
Regina REXX	Regina REXX is a full scripting language with Registry access, event log functions, and OLE automation support.	BATCH/SCRIPT
REGINI.EXE	Command-line utility which makes changes to the Registry based on a script. Good for Setup programs.	COMMAND-LINE
REGKEY.EXE	Supports interactive setting of Logon and FAT file system settings including parsing of AUTOEXEC.BAT for SET/PATH commands.	COMMAND-LINE
REGREAD.EXE	This command-line utility reads the Registry, parses out values, and outputs them to the screen.	COMMAND-LINE
REGREST.EXE	Used in conjunction with regback.exe, this command-line utility will restore registry hives from backup files and is effective upon system reboot. User must have SeRestorePriviledge to execute this command.	COMMAND-LINE
REGSEC.EXE	This command-line utility removes the Everyone group from a Registry key. Removing the Everyone group can enable you to implement stricter and more specific security.	COMMAND-LINE
REGTOGRP.EXE	Creates a Windows NT specific .GRP file in the current directory for each of your Program Manager groups. This file is not compatible with MS-DOS Windows. (Must be used with GRPTOREG.EXE.)	COMMAND-LINE
Remote Access Manager	Remote Access Manager, by virtual motion, enables network managers to manage Remote Access Service (RAS) on a per-user, RAS server, or port basis. You can control RAS resources via LAN or dial-up access. With Remote Access Manager, you can: display RAS server and port status. disconnect RAS sessions from any port. enable or disable RAS privileges for any user.	MULTI-FILE APPLICATION
Remote Console	Remote Console is a client/server application that enables you to run a command-line session remotely, within which you may launch any other application.	
REMOTE.EXE	Command-line utility to provide remote command-line access to start either the Client or Server end of Remote.	COMMAND-LINE
Remote Kill	This service (RKILLSRV.EXE) with both GUI (WRKILL.EXE) and command-line (RKILL.EXE) clients allows a user to enumerate and kill processes on a remote computer. To kill a process remotely with this tool, you must be member of the Administrators group.	COMMAND-LINE /GUI
RESTKEY.EXE	This command-line utility enables you to restore a Registry key from a file.	COMMAND-LINE
RIPROUTE.WRI	This Microsoft Write document explains how you can use Windows NT Server, along with Windows NT Server Multi-Protocol Routing, to connect local area networks (LANs) together or local area networks to wide area networks (WANs) without needing to purchase a dedicated router.	DOCUMENT NT SERVER ONLY
RM.EXE	POSIX command-line utility for file deletion or removal.	COMMAND-LINE
RMDIR.EXE	POSIX command-line utility for directory deletion or removal.	COMMAND-LINE

RMTSHARE.EXE	RMTSHARE.EXE is a command-line utility that allows you to set up or delete shares remotely.	COMMAND-LINE
ROBOCOPY.EXE	A robust file copy command which includes switches for including populated and unpopulated subdirectories, adjusting attributes, setting date and time stamps, establishing wait and retry intervals, establishing exclusion clauses, and moving subdirectories after copy.	COMMAND-LINE
RREGCHG.EXE	This command-line and batch utility creates or changes Registry settings on a remote computer. It is useful for making global Registry changes over a network.	COMMAND-LINE
RSHSVC.EXE	RSHSVC.EXE is the server side for the TCP/IP utility rsh.exe. It works the same way as the UNIX remote Shell Service. RSH clients can access this service from both NT and UNIX machines.	SERVICE
SAVEKEY.EXE	This command-line utility enables you to save a Registry key to a file.	COMMAND-LINE
SC.EXE	This tool provides a way to communicate with the Service Controller (the SERVICES.EXE process) from the command prompt.	COMMAND-LINE
SCANREG.EXE	A Win32 character-based/command-line "Registry GREP" that enables you to search for any string in keynames, valuenames, and/or valuedata in local or remote Registries keys in both Windows NT and Windows 95.	COMMAND-LINE /GUI
SETUPMGR.EXE	Creates an answer file of system and licensing information for unattended product installation/upgrade.	COMMAND-LINE
SCLIST.EXE	This command-line tool can show currently running services, stopped services, or all services on a local or remote computer.	COMMAND-LINE
SCOPY.EXE	Command-line utility which copies files to and from NTFS partitions while keeping file permissions intact. User must have Backup and Restore file security rights on both the source and destination directories. Not compatible with FAT, HPFS or any other non-secured file system.	COMMAND-LINE
SECADD.EXE	This command-line utility enables you to add user permissions to a Registry key.	COMMAND-LINE
SECEDIT.EXE	This GUI security-context editor allows you to modify security privileges of the logged-on user and running processes, and to list the security contexts that are in use.	GUI
SETX.EXE	A command-line utility that offers a batch method for setting environmental variables in the user or machine environment from a variety of sources, without any programming or scripting. Besides taking both the variable and value from the command line, it can also take values from Registry keys and offsets into text files.	COMMAND-LINE
SH.EXE	POSIX utility for creation of a command shell.	COMMAND-LINE
ShareUI	This stand-alone extension of Explorer makes it easier to manage network shares. ShareUI is a special shell folder that allows you to view, add, remove, and configure the properties of network shares for any local or remote machine that you have permission to administer. Network shares are objects that represent shared directories on a computer.	EXPLORER EXTENSION
SHOWACLS.EXE	This command-line utility enumerates access rights for files, folders, and trees. It allows masking to enumerate only specific ACLs.	COMMAND-LINE

SHOWDISK.EXE	This command-line utility reads and displays the Registry Subkey HKEY_LOCAL_MACHINE\SYSTEM\DISK. This Subkey contains information about each of the primary partitions and logical drives defined on the computer. It also identifies which of the primary partitions and logical drives are members of volume sets, stripe sets, mirror sets, and stripe sets with parity.	COMMAND-LINE
SHOWGRPS.EXE	This command-line tool displays group information for a specified user.	COMMAND-LINE
SHUTDOWN.EXE	Third-party utility which allows a user to shutdown a local or remote server with command-line options support.	COMMAND-LINE
SHUTGUI.EXE	SHUTGUI.EXE allows you to remotely shut down or reboot a computer running Windows NT. It can be run either with command-line parameters or without.	COMMAND-LINE /GUI
SLEEP.EXE	Command-line utility which executes a pause for a specified amount of time in seconds. Useful in batch processing.	COMMAND-LINE
SMBTRACE.EXE	Executes an SMB packet trace from the server or redirector. Includes command-line option support.	COMMAND-LINE
SNMPMON.EXE	SNMP Monitor is a utility that can monitor any SNMP MIB variables across any number of SNMP nodes. It can then optionally log query results to any ODBC data source (such as SQL Server), automatically creating any necessary tables. Logging can be enabled for all queries or limited to particular thresholds, and thresholds can be either edge or level triggered.	GUI
SNMPUTIL.EXE	Command-line browsing utility which allows you to get SNMP information from an SNMP host on your network.	COMMAND-LINE
SOON.EXE	SOON.EXE is a command scheduling utility which runs an AT command in the near future. The delay is set in seconds and can run commands locally or remotely.	COMMAND-LINE
SRVANY.EXE	This utility allows running Windows NT applications as services.	COMMAND-LINE
SRVCHECK.EXE	This command-line utility lists the non-hidden shares on an computer running Windows NT and enumerates the users on the ACL's for that share.	COMMAND-LINE
SRVINFO.EXE	This command-line utility displays information about a remote server.	COMMAND-LINE It is included in the Windows NT Server Resource Kit only.
SRVINSTW.EXE	The Service Installation Wizard provides an easy method of installing or deleting services and device drivers. It can connect to and configure services on both local and remote computers.	GUI
SRVMGR.EXE	Windows-based remote server administration tool.	GUI
SU.EXE	SU lets you start a process running as an arbitrary user. It is named after the SU (Switch Users) utility of the UNIX family of operating systems.	COMMAND-LINE
SYSDIFF.EXE	This utility enables you to pre-install applications, including those that do not support scripted installation, as part of an automated setup.	COMMAND-LINE It is included in the Windows NT Server Resource Kit only.
TDISHOW.EXE	Menu-driven command-line utility which allows a user to capture and display TDITRACE buffer information.	COMMAND-LINE

Telnet Server Beta (TELNETD.EXE)	Telnet Server has two components: the service itself (TELNETD.EXE) and an underlying component, the Remote Session Manager (RSM.EXE). The Telnet Server service operates by connecting to the Remote Session Manager component. Remote Session Manager (RSM) is responsible for initiating, terminating, and managing the character-oriented remote telnet session on a given system. RSM affects only the services provided in the Telnet Server service; it does not affect Microsoft's Remote Access Service (RAS), or other layered products.	COMMAND-LINE
TEXTVIEW.EXE	TextViewer provides a graphical interface for quickly viewing text files on local or shared drives. While it provides basic editing and searching capabilities, it is primarily intended for viewing similar files within multiple sub-folders.	GUI
TIMEOUT.EXE	Similar to the DOS "pause" command, timeout.exe will wait a period of time denoted in seconds and then continue running without a key press.	COMMAND-LINE
TIMESERV.EXE	This service sets the system time accurately and keeps Windows NT workstations and servers synchronized with a primary or secondary timesource that you specify. TIMESERV always keeps the computer in sync, even when no one is logged on. The service can be run from either the Services Control Panel or the command prompt.	SERVICE
TIMETHIS.EXE	Executes the command specified by it's arguments and reports its run time in HH:MM:SS.TTT format.	COMMAND-LINE
TIMEZONE.EXE	This command-line utility updates the daylight savings information for a timezone in the Registry.	COMMAND-LINE
TLIST.EXE	The Task List Viewer is a command-line utility that displays a list of tasks, or processes, currently running on the local computer. For each process, it shows the process ID number, process name, and, if the process has a window, the title of that window.	COMMAND-LINE
TLOCMGR.EXE	Telephony Location Manager was written for laptop computer users who use telephone applications, such as Dial-Up Networking, from several locations. It is useful for anyone who changes Telephony API (TAPI) locations-for example, taking a laptop from the office to home, where the computer no longer has to dial a "9" prefix. For a laptop user with a hot-docking setup, this utility will automatically change the TAPI location.	EXPLORER EXTENSION
TOPDESK.EXE	This command along with topdesk.hlp presents a small representation of the virtual desktop showing your current desktop, the home desktop, all visible windows, and optionally, all ghost windows. TopDesk lets you manipulate all of these objects with various keyboard and mouse actions.	GUI
TOUCH.EXE	POSIX utility used to change date and/or time of a file.	COMMAND-LINE
TZEDIT.EXE	Time Zone editor.	GUI
UPTOMP.EXE	A performance and system monitoring utility which upgrades a single-processor system to a multiprocessor system.	COMMAND-LINE
USRMGR.EXE	The Windows NT User Manager utility which provides for the management of accounts, group membership and access permissions.	GUI
USRSTAT.EXE	This command-line utility displays username, fullname, and last login date and time for each user in a given domain.	COMMAND-LINE

USRTOGRP.EXE	Using a text file containing a Domain name on line 1, a Local or Global group name on line 2, and user names on successive lines, this utility will add users to groups in batch.	COMMAND-LINE
VDESK.EXE	VDESK.EXE is a simple desktop switcher that enables you to maintain multiple desktops on a computer running Windows NT Workstation.	GUI
VI.EXE	POSIX text file editor.	COMMAND-LINE
WC.EXE	POSIX utility for 'word count'.	COMMAND-LINE
Web Administration of Windows NT Server	This ISAPI DLL allows limited remote administration of Windows NT Server via HTML browsers (including Internet Explorer 2.0 and later) from Windows, Macintosh and UNIX platforms. Web Administration of Microsoft Windows NT Server is included in the Windows NT Server Resource Kit only and is also available for download from the Microsoft World Wide Web site. This tool does not replace existing administrative tools for Windows NT Server, but rather assists administrators when they do not have access to existing tools-for example, when they are away from their normal administrative workspace. This tool will be particularly useful for Windows NT administrators who are already experienced with the current administrative tools on Windows NT Server 3.51 and 4.0.	MULTI-FILE APPLICATION
WHOAMI.EXE	POSIX utility for identifying active session.	COMMAND-LINE
WINAT.EXE	Command Scheduler can be used to schedule commands on a local or remote computer to occur once or regularly in the future. The Workstation service must be started to use this application.	GUI
WINDIFF.EXE	Windows-based utility showing the differences between two named files or directories.	GUI
WINEXIT.SCR	WINEXIT is a screen saver that logs the current user off after the specified time has elapsed. It is similar to other screen savers and can be configured and tested using the Desktop icon in Control Panel.	SCREEN SAVER
WINMSDP.EXE	WinMsdP is a command-line version of WINMSD.EXE. It provides information about your system configuration and status.	COMMAND-LINE
WINSCHK.EXE	This command-line utility checks name and version-number inconsistencies that may appear in Windows Internet Name Service (WINS) databases, monitors replication activity, and verifies the replication topology in an enterprise network. It is particularly useful for WINS administrators.	COMMAND-LINE
WINSCL.EXE	Command-line utility providing limited NT server administration capabilities via TCP/IP or a named pipe.	COMMAND-LINE
WINSDMP.EXE	Tool which has been designed to take a dump from the WINS database and provide this output in a fixed record file format	COMMAND-LINE
WNTIPCFG.EXE	WNTIPCFG is a graphical version of the IPConfig utility that is shipped with the Windows NT operating system. Use this utility to manage the Internet Protocol (IP) addresses and view IP information for computers that run the TCP/IP protocol.	GUI

THE GLOSSARY

Term	Definition
ACL	Access Control List: A list associated with a file that contains information about which users or groups have permission to access or modify the file.
API	Application Programming Interface: A set of routines that an application program uses to request and carry out lower-level services performed by the computer's OS.
BDC	Backup Domain Controller: In a Windows NT Server domain, a computer running Windows NT Server that receives a copy of the domain's directory database, which contains all account and security policy information for the domain. The copy is synchronized periodically and automatically with the master copy on the PDC. BDC's also authenticate user logons and can be promoted to function as PDC's as needed. Multiple BDC's can exist on a domain.
C2	Class 2: The lowest level of security in the U.S. National Computer Security Center's hierarchy of criteria for trusted computer systems, requiring user logon with password and a mechanism for auditing. The C2 level is outlined in the Department of Justice's Orange Book.
CD-ROM	Compact Disk Read-Only Memory: A form of storage characterized by high capacity (roughly 650 megabytes) and the use of laser optics rather than magnetic means for reading data. Although CD-ROM drives are strictly read-only, they are similar to CD-R drives (write once, read many), optical WORM devices, and optical read-write drives.
CLI	Command-Line Interface
COTS	Commercial Off-The-Shelf: A software product installed with its default configuration.
CPU	Central Processing Unit: The computational and control unit of a computer. The central processing unit is the device that interprets and executes instructions. Mainframes and early minicomputers contained circuit boards full of integrated circuits that implemented the central processing unit. Single-chip central processing units, called microprocessors, made possible personal computers and workstations. Examples of single-chip central processing units are the Motorola 68000, 68020, and 68030 chips and the Intel 8080, 8086, 80286, 80386, and i486 chips. The central processing unit--or microprocessor, in the case of a microcomputer--has the ability to fetch, decode, and execute instructions and to transfer information to and from other resources over the computer's main data-transfer path, the bus. By definition, the central processing unit is the chip that functions as the "brain" of a computer. In some instances, however, the term encompasses both the processor and the computer's memory or, even more broadly, the main computer console (as opposed to peripheral equipment).
DAC	Discretionary Access Control: Allows the network administrator to allow some users to connect to a resource or perform an action while preventing other users from doing so.
DHCP	Dynamic Host Configuration Protocol: A TCPIP protocol that enables a network connected to the Internet to assign a temporary IP address to a host automatically when the host connects to the network.
DLL	Dynamic Link Library: A feature of the Microsoft Windows family of operating systems and OS2 that allows executable routines to be stored separately as files with DLL extensions and to be loaded only when needed by a program. A dynamic-link library has several advantages. First, it does not consume any memory until it is used. Second, because a dynamic-link library is a separate file, a programmer can make corrections or improvements to only that module without affecting the operation of the calling program or any other dynamic-link library. Finally, a programmer can use the same dynamic-link library with other programs.
DNS	Domain Name Service: The Internet utility that implements the Domain Name System. DNS servers, maintain databases containing the addresses and are accessed transparently to the user.
DOD	Department Of Defense: The military branch of the United States government. The Department of Defense developed ARPANET, the origin of today's Internet and MILNET, through its Advanced Research Projects Agency.
ERD	Emergency Repair Disk
GB	GigaByte: 1,024 megabytes (1,024 × 1,048,576, [2^{30}] bytes) or one thousand megabytes (1,000 × 1,048,576 bytes).

HDD	Hard Disk Drive: A device containing one or more inflexible platters coated with material in which data can be recorded magnetically, together with their read/write heads, the head-positioning mechanism, and the spindle motor in a sealed case that protects against outside contaminants. The protected environment allows the head to fly 10 to 25 millionths of an inch above the surface of a platter rotating typically at 3600 to 7200 rpm; therefore, much more data can be stored and accessed much more quickly than on a floppy disk. Most hard disks contain from two to eight platters.
IIS	Internet Information Server: Microsoft's brand of Web server software, utilizing Hypertext Transfer Protocol to deliver World Wide Web documents. It incorporates various functions for security, allows for CGI programs, and also provides for Gopher and FTP servers.
INFOSEC	INFOrmation SECurity
KB	KiloByte: A data unit of 1,024 bytes.
LAN	Local Area Network: A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. LANs commonly include microcomputers and shared resources such as laser printers and large hard disks. The devices on a LAN are known as nodes, and the nodes are connected by cables through which messages are transmitted. See also baseband network, broadband network, bus network, collision detection, communications protocol, contention, CSMACD, network, ring network, star network, token bus network, token passing, token ring network.
MB	MegaByte: 1,048,576 bytes (2^{20}); sometimes interpreted as 1 million bytes.
MHZ	MegaHertZ: A measure of frequency equivalent to 1 million cycles per second.
MS-DOS	MicroSoft Disk Operating System: A single-tasking, single-user operating system with a command-line interface, released in 1981, for IBM PCs and compatibles. MS-DOS, like other operating systems, oversees operations such as disk input and output, video support, keyboard control, and many internal functions related to program execution and file maintenance.
NetBEUI	NetBios Extended User Interface: An enhanced NetBIOS protocol for network operating systems, originated by IBM for the LAN Manager server and now used with many other networks.
NetBIOS	Network Basic Input Output System: An API that can be used by application programs on a local area network consisting of IBM and compatible microcomputers running MS-DOS, OS2, or some version of UNIX. Primarily of interest to programmers, NetBIOS provides application programs with a uniform set of commands for requesting the lower-level network services required to conduct sessions between nodes on a network and to transmit information back and forth.
NOS	Network Operating Systems: An operating system installed on a server in a local area network that coordinates the activities of providing services to the computers and other devices attached to the network. Unlike a single-user operating system, a network operating system must acknowledge and respond to requests from many workstations, managing such details as network access and communications, resource allocation and sharing, data protection, and error control.
NTFS	New Technology File System: An advanced file system designed for use specifically with the Windows NT operating system. It supports long filenames, full security access control, file system recovery, extremely large storage media, and various features for the Windows NT POSIX subsystem. It also supports object-oriented applications by treating all files as objects with user-defined and system-defined attributes.
NTS	Windows NT Server: A superset of Windows NT Workstation, Windows NT Server provides centralized management and security, fault tolerance, and additional connectivity.
NTW	Windows NT Workstation: The portable, secure, 32-bit, preemptive multitasking member of the Microsoft Windows operating system family.
ODBC	Open DataBase Connectivity: In the Microsoft WOSA structure, an interface providing a common language for Windows applications to gain access to a database on a network
OS	Operating System: The software that controls the allocation and usage of hardware resources such as memory, CPU time, disk space, and peripheral devices. The operating system is the foundation on which applications are built. Popular operating systems include Windows 95, Windows NT, Mac OS, and UNIX. Also called executive.
PDC	Primary Domain Controller: In a Windows NT Server domain, the computer running Windows NT Server that authenticates domain logons and maintains the directory database for a domain. The PDC tracks changes made to accounts of all computers on a domain. It is the only computer to receive these changes directly. A domain has only one PDC.

POSIX	Portable Operating System Interface for uniX: An IEEE standard that defines a set of operating-system services. Programs that adhere to the POSIX standard can be easily ported from one system to another. POSIX was based on UNIX system services, but it was created in a way that allows it to be implemented by other operating systems.
PPTP	Point-to-Point Tunneling Protocol: A specification for virtual private networks in which some nodes of a local area network are connected through the Internet.
RAM	Random Access Memory: Semiconductor-based memory that can be read and written by the central processing unit (CPU) or other hardware devices. The storage locations can be accessed in any order. Note that the various types of ROM memory are capable of random access, but cannot be written to. The term RAM, however, is generally understood to refer to volatile memory that can be written to as well as read.
RAS	Remote Access Service: Windows software that allows a user to gain remote access to the network server via a modem.
RISC	Reduced Instruction Set Computer: A microprocessor design that focuses on rapid and efficient processing of a relatively small set of simple instructions that comprises most of the instructions a computer decodes and executes. RISC architecture optimizes each of these instructions so that it can be carried out very rapidly--usually within a single clock cycle. RISC chips thus execute simple instructions more quickly than general-purpose CISC (complex instruction set computing) microprocessors, which are designed to handle a much wider array of instructions. They are, however, slower than CISC chips at executing complex instructions, which must be broken down into many machine instructions that RISC microprocessors can perform. Families of RISC chips include Sun Microsystems' SPARC, Motorola's 88000, Intel's i860, and the PowerPC developed by Apple, IBM, and Motorola.
RPC	Remote Procedure Call: A message-passing facility that allows a distributed application to call services available on various machines in a network. Used during remote administration of computers.
SP	Service Pack
SQL	Structured Query Language: A database sub-language used in querying, updating, and managing relational databases.
TCP/IP	Transmission Control Protocol/Internet Protocol: A protocol developed by the Department of Defense for communications between computers. It is built into the UNIX system and has become the de facto standard for data transmission over networks, including the Internet.
UDP	User Datagram Protocol: The connectionless protocol within TCPIP that corresponds to the transport layer in the ISOOSI model. UDP converts data messages generated by an application into packets to be sent via IP but does not verify that messages have been delivered correctly. Therefore, UDP is more efficient than TCP, so it is used for various purposes, including SNMP; the reliability depends on the application that generates the message.
UID	User IDentifier
UPS	Un-interruptable Power Source: A device, connected between a computer (or other electronic equipment) and a power source (usually an outlet receptacle), that ensures that electrical flow to the computer is not interrupted because of a blackout and, in most cases, protects the computer against potentially damaging events, such as power surges and brownouts. All UPS units are equipped with a battery and a loss-of-power sensor; if the sensor detects a loss of power, it switches over to the battery so that the user has time to save his or her work and shut off the computer.
URL	Uniform Resource Locator: An address for a resource on the Internet. URLs are used by Web browsers to locate Internet resources. An URL specifies the protocol to be used in accessing the resource (such as http: for a World Wide Web page or ftp: for an FTP site), the name of the server on which the resource resides (such as www.whitehouse.gov), and, optionally, the path to a resource (such as an HTML document or a file on that server).
VGA	Video Graphics Adapter: A video adapter that duplicates all the video modes of the EGA (Enhanced Graphics Adapter) and adds several more.
WINS	Windows Internet Naming Service: A Windows NT Server method for associating a computer's host name with its address. Also called INS, Internet Naming Service.
WOSA	Windows Open System Architecture: A set of application programming interfaces from Microsoft that is intended to enable Windows applications from different vendors to communicate with each other, such as over a network. The interfaces within the WOSA standard include ODBC, the Messaging API, the API, Winsock, and Microsoft RPC.

THE ACKNOWLEDGEMENTS

This document represents the effort of many individuals on many different levels. Not only myself, but also numerous authors of other related NT Security documentation have made this culmination of information possible.

Contributors to this document

Acknowledging	Role	Contribution
Eric Schultz bealls@ix.necom.com	contributor	Detailed subject matter & guidance for document specifics
Robert Davis rdavis@lucentncg.com	contributor	Comments, suggestions and details based upon his document
Franz Katterbach katterbach@rad.rwth-aachen.de	contributor	Password sniffing via NetWare .DLL information
Gary Griffith ggriffth@netdox.xom	contributor	Auto-share removal details
James Raykowski jimrski@cts.com	contributor	Detailed SP3 default NTFS ACL information
David Bones dbonnes@ozemail.com.au	collaborator	Shared documents on NT Security
David Furey dave@cia.com.au	editor	Programmer of the companion application & editor
Ellen Cliggot ellenjc@ix.netcom.com	technical document editor	Freelance technical writer and editor

Contributing efforts of previous works

Acknowledging	Role	Project
Robert Davis	author	Securing Windows NT Installation
H Morrow Long James Mohr Neon Surge	contributors	
Capt Daniel Galik Lt Gib Winter	project impetus and funding	Secure Windows NT Installation and Configuration Guide
Raymond Galloni Jean-Paul Otin Russell Reopell Lara Sosnosky	principle authors / researchers	
Linda Chock Michelle Gosselin Thomas Gregg Kenneth Jones Carol Oake Harvey Rubinovitz	guidance and editing	

THE AUTHOR

Micheal Espinola Jr is a 25 year old Network Administrator who works in Lexington, Massachusetts for a multi-million dollar software company.

During his high school years, he was associated with the predominant hackers of the Boston area. Most, like Micheal, are now using their skills in the work force as security advisors for telephone and computer companies. A few have continued the tradition and have far surpassed all others to form the now infamous L0pht Heavy Industries.

Now working on the other side of the fence, he strives to continue the battle for information security. He recognizes that information is power. More importantly now than any other time in human history. However, today he fights to keep that knowledge from being exploited by malicious hackers and industrial espionage. He treads both sides of the fence to keep ahead of the game, all the while sharing freely that knowledge with anyone that has a need for it.

Micheal currently lives on a lake in New Hampshire and unwinds from a hard days work by racing around town in the 1980 Camaro Z28 he is currently restoring.

"I don't practice Santeria, I ain't got no crystal ball …
… I had a million dollars, but I spent it all!"

- Sublime (rip)

"Soaring higher with every treason …
… never justify, never reason."

- Letters to Cleo

THE DISCLAIMER

MICHEAL ESPINOLA JR AND/OR HIS RESPECTIVE DISTRIBUTERS OF THIS DOCUMENT MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THIS DOCUMENT AND RELATED DOCUMENTS REFERENCED IN THIS DOCUMENT FOR ANY PURPOSE.

THIS DOCUMENT AND RELATED DOCUMENTS REFERENCED ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICHEAL ESPINOLA JR AND/OR HIS RESPECTIVE DISTRIBUTERS HEREBY DISCLAIM ALL WARRANTIES.

IN NO EVENT SHALL MICHEAL ESPINOLA JR AND/OR HIS RESPECTIVE DISTRIBUTERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION AVAILABLE FROM THIS DOCUMENT.

THIS DOCUMENT AND RELATED DOCUMENTS REFERENCED IN THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. MICHEAL ESPINOLA JR AND/OR HIS RESPECTIVE DISTRIBUTERS MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE DOCUMENT AND/OR THE RELATED DOCUMENTS REFERENCED HEREIN AT ANY TIME.

Microsoft, the Microsoft logo, Win32 and Windows NT are trademarks of:

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399